Firepower System Release Notes

Version 6.0.1
First Published: March 20, 2016
Last Updated: March 30, 2018

These release notes are valid for Version 6.0.1 of the Firepower System. Even if you are familiar with the update process, make sure you thoroughly read and understand these release notes, which describe supported platforms, new and changed features and functionality, management platform-managed device compatibility, and known and resolved issues. They also contain detailed information on prerequisites, warnings, and specific installation instructions.

Tip To access the full documentation for the Firepower System, see the documentation roadmap at http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html.

Note: To reduce the time to update to Version 6.0.1, install the Version 6.0.1 Pre-Installation Package before you update. For more information, see the *FireSIGHT System Release Notes for Version 6.0.1 Pre-Installation Package*.

For more information, see the following sections:

Supported Platforms and Compatibility

Supported platforms, minimum originating versions, and operating systems vary by version. For more information, see:

Supported Platforms

You can run Version 6.0.1 on the platforms specified in the following table. For minimum Firepower System version requirements, see Firepower Version Requirements for Updating to Version 6.0.1, page 15.

Table 1 Platform Support in Version 6.0.1

Supported platforms in Version 6.0.1	Capability in Version 6.0.1	Other requirements to run Version 6.0.1
Firepower Management Center (the MC750, MC1500, MC3500, MC2000, and the MC4000)	management	■ MC750 requires two 4GB dual in-line memory modules (DIMM)
64-bit Firepower Management Center Virtual	management	hosted on: ■ VMware vSphere Hypervisor/VMware ESXi 5.1 ■ VMware vSphere Hypervisor/VMware ESXi 5.5 ■ VMware vCloud Director 5.1
Firepower 7000 Series and 8000 Series (the 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8380, and the AMP8390)	managed device	n/a
Note: Cisco ASA with Cisco ASA with FirePOWER Services (the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, AS A5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X	managed device	running: ■ ASA version 9.4(x) *No captive portal* ■ ASA Version 9.5(1.5) *No captive portal* ■ ASA Version 9.5(2) ■ ASA Version 9.5(3) ■ ASA Version 9.6(x)
ASA Firepower software module managed via ASDM (the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X	management	running: ■ ASA Version 9.5(1.5) *No captive portal* ■ ASA Version 9.5(2) ■ ASA Version 9.5(3) ■ ASA Version 9.6(x) ■ ASDM version 7.5.2(153), or 7.6.1
NGIPSv (virtual managed device)	managed device	hosted on: ■ VMware vSphere Hypervisor/VMware ESXi 5.1 ■ VMware vSphere Hypervisor/VMware ESXi 5.5 ■ VMware vCloud Director 5.1

Table 1 Platform Support in Version 6.0.1

Supported platforms in Version 6.0.1	Capability in Version 6.0.1	Other requirements to run Version 6.0.1
Cisco ASA with Firepower Threat Defense (the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, and the ASA 5555-X)	managed device	The following running ROMMON version 1.1.8 or later: the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X
Firepower 4100 series with Threat Defense (the 4110, 4120, and the 4140)	managed device	running: ■ FXOS version 1.1.4
Firepower 9300 with Threat Defense	managed device	running: ■ FXOS version 1.1.4
Firepower Threat Defense Virtual: VMware and Amazon Web Services (AWS)	managed device	hosted on: ■ VMware vSphere Hypervisor/VMware ESXi 5.1 ■ VMware vSphere Hypervisor/VMware ESXi 5.5 ■ VMware vCloud Director 5.1Amazon Elastic Compute Cloud (EC2) ■ Amazon Virtual Private Cloud (VPC)

Management Platform-Managed Device Compatibility

Management capability varies by version. The following tables detail available management platforms and the devices that those platforms can manage:

Table 2 Management Platform-Compatibility by Management Platform

Supported management platforms	What can you manage using this management platform?
Firepower Management Centers (the MC750, MC1500, MC3500, MC2000, and the MC4000)	All of the following, running at least Version 5.4.0.2 or later: ■ Firepower 7000 Series and 8000 Series (the 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8380, and the AMP8390) ■ NGIPSv (virtual managed devices) ■ Cisco ASA with Firepower Services (the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, and the ASA 5585-X-SSP-60) All of the following, Running Version 5.4.1.1 or later: ■ Cisco ASA with Firepower Services (the ASA 5506X- ASA 5506H-X, ASA 5506W-X, ASA 5508-X, and the ASA 5516-X) All of the following, running Version 6.0.1: ■ Firepower 7000 Series and 8000 Series (the 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8380, and the AMP8390) ■ NGIPSv (virtual managed devices) ■ Cisco ASA with Firepower Services (the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, and the ASA 5585-X-SSP-60) ■ Cisco ASA with Firepower Threat Defense (the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, and the ASA 5555-X) ■ Firepower 4100 Series with Threat Defense (4110, 4120, and the 4140) ■ Firepower 9300 with Threat Defense ■ Firepower Threat Defense Virtual: VMware and Amazon Web Services (AWS)
ASDM Version 7.6.1	All of the following, running ASA Version 9.6(1) with Version 6.0.1: ■ Cisco ASA with Firepower Services (the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X)
ASDM Version 7.5.2	All of the following, running ASA Version 9.5(2) with Version 6.0.1: ■ Cisco ASA with Firepower Services (the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X)

Table 2 Management Platform-Compatibility by Management Platform

Supported management platforms	What can you manage using this management platform?
64-bit Firepower Management Centers Virtual	All of the following, running at least Version 5.4.0.2 or later: ■ Firepower 7000 Series and 8000 Series (the 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8380, and the AMP8390) ■ NGIPSv (virtual managed devices) ■ Cisco ASA with Firepower Services (the ASA 5516-X, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, and the ASA 5585-X-SSP-60) All of the following, Running Version 5.4.1.1 or later: ■ Cisco ASA with Firepower Services (the ASA 5506X- ASA 5506H-X, ASA 5506W-X, ASA 5508-X, and the ASA 5516-X) All of the following, running Version 6.0.1: ■ Firepower 7000 Series and 8000 Series (the 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8380, and the AMP8390) ■ NGIPSv (virtual managed devices) ■ Cisco ASA with Firepower Services (the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, and the ASA 5585-X-SSP-60) ■ Cisco ASA with Firepower Threat Defense (the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, and the ASA 5555-X) ■ Firepower 4100 Series with Threat Defense (4110, 4120, and the 4140) ■ Firepower 9300 Series with Threat Defense ■ Firepower Threat Defense Virtual: VMware and Amazon Web Services (AWS)

Table 3 Management Platform-Managed Device Compatibility by Managed Device

Supported Managed Devices	What can you use to manage this device?
Firepower 7000 Series and 8000 Series (the 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8380, and the AMP8390)	All of the following, running Version 6.0.1: ■ Firepower Management Centers (the MC750, MC1500, MC3500, MC2000, and the MC4000) ■ 64-bit Firepower Management Centers Virtual
Cisco ASA with FirePOWER Services (the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, and the ASA 5585-X-SSP-60)	All of the following, running Version 6.0.1: ■ Firepower Management Centers (the MC750, MC1500, MC3500, MC2000, and the MC4000) ■ 64-bit Firepower Management Centers Virtual ■ Cisco ASA managed by ASDM (the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, and the ASA 5585-X-SSP-60)
NGIPSv (virtual managed devices)	All of the following, running Version 6.0.1: ■ Firepower Management Centers (the MC750, MC1500, MC3500, MC2000, and the MC4000) ■ 64-bit virtual Firepower Management Centers
Cisco ASA with Firepower Threat Defense (the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, and the ASA 5555-X)	All of the following, running Version 6.0.1: ■ Firepower Management Centers (the MC750, MC1500, MC3500, MC2000, and the MC4000) ■ 64-bit Firepower Management Centers Virtual
Firepower 4100 Series with Threat Defense (the 4110, 4120, and the 4140)	All of the following, running Version 6.0.1: ■ Firepower Management Centers (the MC750, MC1500, MC3500, MC2000, and the MC4000) ■ 64-bit Firepower Management Centers Virtual ■ Cisco FXOS Firepower Chassis Manager, 1.1.4, also manages some device functionality not available on the Firepower Management Center.
Firepower 9300 Series with Threat Defense	All of the following, running Version 6.0.1: ■ Firepower Management Centers (the MC750, MC1500, MC3500, MC2000, and the MC4000) ■ 64-bit Firepower Management Centers Virtual ■ Cisco FXOS Firepower Chassis Manager, 1.1.4, also manages some device functionality not available on the Firepower Management Center.
Firepower Threat Defense Virtual: VMware and Amazon Web Services (AWS)	All of the following, running Version 6.0.1: ■ Firepower Management Centers (the MC750, MC1500, MC3500, MC2000, and the MC4000) ■ 64-bit Firepower Management Centers Virtual

New Features and Functionality

This section of the release notes summarizes the new and updated features and functionality included in Version 6.0.1 of the Firepower System:

New Features

The following features are introduced in Version 6.0.1:

Fully Integrated, Threat-Focused Next-Generation Firewall

Most next-generation firewalls (NGFWs) focus heavily on enabling application control, but little on their threat defense capabilities. To compensate, some NGFWs try to supplement their first-generation intrusion prevention with a series of non-integrated add-on products. However, this approach does little to protect your business against the risks posed by sophisticated attackers and advanced malware. Further, once you do get infected, they offer no assistance in scoping the infection, containing it, and remediating quickly.

The Cisco Firepower™ Next-Generation Firewall (NGFW) is the industry's first fully integrated, threat-focused NGFW. It delivers comprehensive, unified policy management of firewall functions, application control, threat prevention, and advanced malware protection from the network to the endpoint.

Firepower Threat Defense

The Firepower Threat Defense software package can be deployed on Cisco Firepower 4100 and 9300 appliances to provide a performance and density optimized NGFW security platform for Internet edge and other high-performance environments. Firepower Threat Defense functionality added in this release includes device and interface management, routing, NAT, and device high availability, in addition to support for the full Firepower NGIPS offering.

This release introduces support for Firepower Threat Defense on the Firepower 4100 Series and the Firepower 9300, as well as on the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X.

Firepower 4100 Series

Stop more threats with our fully integrated next-generation firewall (NGFW) platform. The Firepower 4100 Series' 1-rack-unit size is ideal at the Internet edge and in high-performance environments. It shows you what is happening on your network, detects attacks earlier so you can act faster, and reduces management complexity.

Firepower 9300 Series

This carrier-grade platform is ideal for data centers and other high-performance settings that require low latency and high throughput. Deliver scalable, consistent security to workloads and data flows across physical, virtual, and cloud environments. With tightly integrated services, the Firepower 9300 lowers costs and supports open, programmable networks. The Firepower 9300 Series offers up to 1.2 Tbps clustered throughput, 10/40/100 Gb network interfaces, up to 57 million concurrent connections with application control, and 500,000 new connections per second. Available features and services include a stateful firewall, application visibility and control, NGIPS, advanced malware protection, reputation-based URL filtering, and DDoS mitigation.

Updated Terminology

The terminology used in Version 6.0.1 may differ from the terminology used in previous releases. For more information, see the *Firepower Compatibility Guide*.

Updated Documentation

To access the full documentation for the Firepower System, see the documentation roadmap at http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html. In Version 6.0.1, the following documents were updated to reflect the addition of new features and changed functionality and to address reported documentation issues:

- *Firepower Management Center Configuration Guide*
- *Firepower Management Center Online Help*
- *Firepower Management Center Hardware Installation Guide*
- *Firepower Management Center Virtual Quick Start Guide for the AWS Cloud*
- *Cisco Firepower Threat Defense Getting Started Guide for the ASA*
- *Firepower Threat Defense 4100 Series Quick Start Guide*
- *Firepower Threat Defense 9000 Series Quick Start Guide*
- *Cisco FXOS Firepower Chassis Manager Configuration Guide*
- *Firepower Threat Defense Virtual Quick Start Guide for the AWS Cloud*
- *Firepower Threat Defense Virtual Quick Start Guide for VMware*
- *Cisco Firepower Threat Defense Virtual for VMware Deployment*

The documentation updated for Version 6.0.1 contains the following errors:

- The *Firepower Management Center Configuration Guide* incorrectly states that Cisco does not recommend enabling more than one non-SFRP IP address on a 7000 or 8000 Series device high availability pair's routed or hybrid interface where one SFRP IP address is already configured. The system does not perform NAT if a 7000 or 8000 Series device high availability pair experience failover while in standby mode.
- The *Firepower Management Center Configuration Guide* does not reflect that in a multidomain deployment, when you create a DNS policy, the Descendant Whitelists for DNS rule and Descendant Blacklists for DNS rule are disabled by default. You can enable each rule by editing them.

Note: The online help content may differ from the *Firepower Management Center Configuration Guide* content. The *Firepower Management Center Configuration Guide* content is updated more regularly than the online help.

Features and Changed Functionality Introduced in Previous Versions

Functionality described in previous versions may be superseded by other new functionality or updated through resolved issues.

Version 6.0

The following features and functionality were updated in Version 6.0:

Expanded Threat Protection

URL and DNS-based Security Intelligence

New Security Intelligence feeds based on URLs and Domain Name System (DNS) servers are provided to enhance the existing IP-based Security Intelligence capability. Currently, IP-based intelligence is used to control access to known malware, phishing, command & control, and Bot sites. New attack methods designed to defeat IP-based intelligence (e.g., fast flux) abuse DNS load balancing features in an effort to hide the actual IP address of a malicious server. While the IP addresses associated with the attack are frequently swapped in and out, the domain name will rarely change. The URL-based intelligence will supplement the IP-based intelligence in addressing this kind of attack, and the DNS-based intelligence will help identify known DNS servers that are complicit in these kinds of attacks. Access control policies can be created using these new intelligence feeds and new dashboards provide visibility and analysis. In addition, both URL-based and DNS-based Security Intelligence events will also feed in to the Indications of Compromise (IoC) correlation feature. These new feeds are provided through regular updates from the Cisco Talos Security Intelligence and Research Group and, like the IP-based Security Intelligence feature, are part of the base product and do not require a separate license.

DNS Inspection and Sinkholes

The same way that attackers use the SSL protocol to hide their activity, attackers use the DNS protocol with the same intentions. For that reason, and as another way to address fast flux-type attacks, the Firepower system provides the ability to intercept DNS traffic requests and take appropriate action based on the policy setting. A DNS policy allows for requests to known command & control, spam, phishing, etc., sites to be blocked, to return a `Domain Not Found` message, or have the traffic directed to a pre-configured sinkhole. This last option routes the traffic directly through the Firepower managed device and gives information about the endpoint that could result in an IoC alert.

Enhanced Network Visibility and Control

SSL Decryption for Cisco ASA with FirePOWER Services Managed Via ASDM

Cisco's next-generation firewall (NGFW), Cisco ASA with FirePOWER Services, now has the ability to locally manage SSL communications and decrypt the traffic before performing attack, application, and malware detection against it. This is the same capability we introduced in Version 5.4 for Cisco's Firepower next-generation IPS (NGIPS) appliances. SSL decryption can be deployed in both passive and inline modes, and supports HTTPS and StartTLS-based applications (e.g., SMTPS, POP3S, FTPS, IMAPS, TelnetS). Decryption policies can be configured to exert granular control over encrypted traffic logging and handling, such as limiting decryption based on URL categories to enforce privacy concerns. It also provides the ability to block self-signed encrypted traffic, or on SSL version, specific Cipher Suites, and/or unapproved mobile devices.

Support for OpenAppID-Defined Applications

OpenAppID is Cisco's open source, application-focused detection language that enables users to create, share and implement new application detection signatures for custom, localized, and cloud applications, without being dependent upon a NGFW vendor's release cycle or roadmap. In Version 6.0, the Firepower application detection engine that identifies and controls access to over 3,000 applications has been enhanced to recognize OpenAppID-defined applications. In the same way that Snort was an effort to open source the intrusion detection game, OpenAppID is a way to open source the application detection game. Support for OpenAppId-defined applications demonstrates Cisco's commitment to the open source initiatives and the flexibility that it provides to our customers.

Captive Portal and Active Authentication

In order to provide better visibility in mapping users to IP addresses and their associated network events, the Captive Portal and Active Authentication feature can be configured to require users to enter their credentials when prompted through a browser window. The mapping also allows policies to be based on a user or group of users. This feature supplements the existing Sourcefire User Agent (SUA) integration with Active Directory to address non-Windows environments, BYOD users, and guests.

Note: Cisco ASA with FirePOWER Services running ASA Version 9.5(2) and ASA Version 9.5(3) do not support the Captive Portal and Active Authentication feature.

Integration with Cisco Identity Services Engine (ISE)

The integration with Cisco ISE enhances the user identity data available to the system to use in analysis and policy control. By subscribing to Cisco's Platform Exchange Grid (PxGrid), the Firepower Management Center is able to download additional user data, device type data, device location data, and Security Group Tags (SGTs —a method used by ISE to provide network access control). Beyond the added visibility into the users on your network, this data is also actionable intelligence because it extends the control you can provide by creating policies based on SGTs, or on device type, or any of the other information provided by ISE.

Note: In Version 6.0, you cannot use ISE to automatically quarantine an infected endpoint. This functionality will be added in a later release.

Improved Threat Defense Against Advanced Persistent Threats

Local Malware Checks

This feature provides the ability to identify popular/common malware directly on the Firepower appliance, and reduces the need to send files for dynamic analysis (sandboxing), either in the cloud or on-prem (see Intergration with AMP Threat Grid). Using high-fidelity ClamAV signatures, files whose SHA-256 lookup return a disposition of `Unknown` will be analyzed locally on the Firepower appliance to identify common characteristics associated with malware, reducing the need for dynamic analysis.

File Property Analysis

Because certain file types support nested content that can be used to hide malware, this feature provides local analysis of files to determine the viability of malware hidden within. For example, a PDF file can contain different types of files nested inside the file. A file composition report is then run that identifies if nested data exists within the file, what file types those nested files represent, and how likely each nested file is to contain malware. Based on this information, you can choose whether or not to send the file on for dynamic analysis.

Integration with AMP Threat Grid

Cisco's acquisition of ThreatGrid in June 2014 increased our abilities in helping our customers address advanced persistent threats, and that technology has now been fully integrated in Firepower v6.0. AMP Threat Grid now provides our sandboxing capabilities in the cloud when using our **AMP for Firepower** option. Files sent to the cloud for dynamic analysis are securely analyzed and correlated against hundreds of millions of other analyzed malware artifacts to provide a global view of malware attacks, campaigns, and their distribution. Detailed reports identify key behavioral indicators and determine threat scores for faster prioritization and recovery from advanced attacks.

In addition, we have greatly expanded the file types we support for automatic dynamic analysis from just executable files to include PDF and Office documents.

Expanded Management Functionality

Multiple Domain Management

To address the service provider market which must manage separate customer environments, as well as enterprises with acquisitions (resulting in overlapping IP addresses) or geographic business units that need to be managed separately, the Firepower Management Center now has the ability to create multiple management domains. These domains (up to 50) enable separate management environments and are administered using granular role-based access control (RBAC). Each domain provides separate event data, reporting, and network maps.

Policy Hierarchy and Inheritance

To support multiple domain management and make policy administration more efficient, Version 6.0 provides the ability to create a hierarchy of policies. Global policies (e.g., access control) can be established that will apply to all management environments. A policy hierarchy can then be constructed underneath the global policy level to represent different environments, different companies, different business units, or different parts of the organization. Each of these policy environments will inherit the policies of the hierarchy above it, allowing for more consistent and efficient policy management.

Expanded ASDM Management Availability

Cisco's Adaptive Security Device Manager (ASDM) is the local management feature for Cisco ASA with FirePOWER Services. It was introduced as part of the Cisco ASA 5506-X, ASA 5508-X, and ASA 5516-X appliances. With Firepower v6.0, ASDM is now available on the remaining Cisco ASA with FirePOWER Services appliances (ASA 5512-X / ASA 5515-X / ASA 5525-X / ASA 5545-X / ASA 5555-X / ASA 5585-X).

- You cannot compare policies on the following pages: the NAT Policy page, the Platform Settings page, and the SSL Policy page.
- Version 6.0 does not support AMP for Firepower signature lookups with the private AMP cloud. In Version 6.0, the system automatically submits SHA-256 signatures to the public AMP cloud. If you have a private AMP cloud and are receiving events from endpoints, the Version 6.0 Firepower Management Center will continue to receive those events without any additional changes to your configuration.
- Syslog messages for connection events now populate information for the following fields: HTTP Referrer, User Agent, and Referenced Host.
- Version 6.0 does not support Discovery Event Health Monitoring.)
- You can now edit Automatic Application Bypass (AAB) settings on Cisco ASA with FirePOWER Services.

Before You Begin: Important Update and Compatibility Notes

Before you begin the update process for Version 6.0.1, you should familiarize yourself with the behavior of the system during the update process, as well as with any compatibility issues or required pre- or post-update configuration changes.

Note: To reduce the time to update to Version 6.0.1, install the Version 6.0.1 Pre-Installation Package before you update. For more information, see the *FireSIGHT System Release Notes for Version 6.0.1 Pre-Installation Package*.

Caution: Cisco strongly recommends you perform the update in a maintenance window or at a time when the interruption will have the least impact on your deployment.

For more information, see the following sections:

Configuration and Event Backup Guidelines

Before you begin the update, Cisco strongly recommends that you delete or move any backup files that reside on your appliance, then back up current event and configuration data to an external location.

Use the Firepower Management Center to back up event and configuration data for itself and the devices it manages. For more information on the backup and restore feature, see the *Firepower Management Center Configuration Guide*.

Version 6.0.1 does not support AMP for Firepower signature lookups with the private AMP cloud. In Version 6.0, the system automatically submits SHA-256 signatures to the public AMP cloud. If you have a private AMP cloud and are receiving events from endpoints, the Version 6.0 Firepower Management Center will continue to receive those events without any additional changes to your configuration.

Note: The Firepower Management Center purges locally stored backups from previous updates. To retain archived backups, store the backups externally.

Disk Performance Management and Longevity on Firepower 4100 Devices

If you have a Firepower 4100 series device running Firepower Threat Defense, we recommend that you update to the latest version of the software (and at least Version 6.1.0) to take advantage of software updates that enhance disk management performance and disk longevity.

Firepower Management Center High Availability in Version 6.0.x

Although the configuration options for Firepower Management Center high availability appear in the Integration page of the user interface, high availability is not supported for Firepower Management Centers in this release.

Do not attempt to place Firepower Management Centers into high availability.

Traffic Flow and Inspection During the Update

When you update your sensing devices, traffic either drops throughout the update or traverses the network without inspection depending on how your sensing devices are configured and deployed: routed or transparent, inline vs passive, bypass mode settings, and so on. We strongly recommend performing the update in a maintenance window or at a time when the interruptions will have the least impact on your deployment.

Note: When you update 8000 Series clusters or stack pairs, the system performs the update one device at a time to avoid traffic interruption. When you update clustered Cisco ASA with FirePOWER Services devices, apply the update one device at a time, allowing the update to complete before updating the second device.

This section discusses traffic behavior during the following update stages:

- The update itself, including related reboots
- FXOS updates on clustered Firepower Threat Defense, devices
- Configuration deployments after the update

Traffic Behavior During the Update

The following table describes how updates, including related device reboots, affect traffic flow for different deployments. Note that appliances do not perform switching, routing, NAT, and VPN during the update process, regardless of how you configure any inline sets.

Table 4 Update Traffic Behavior

Device	Deployment	Traffic Behavior
Firepower Threat Defense, Firepower Threat Defense Virtual	inline; routed, transparent (including EtherChannel, redundant, transparent)	dropped
	inline in tap mode	egress packet immediately, copy not inspected
	passive	uninterrupted, not inspected

Table 4 Update Traffic Behavior

Device	Deployment	Traffic Behavior
7000 and 8000 Series	inline with optional hardware bypass module, bypass enabled **(Bypass Mode**: **Bypass**)	passed without inspection Network traffic is interrupted briefly at two points: ■ At the beginning of the update process, as link goes down and up (flaps) and the network card switches into hardware bypass. ■ After the update finishes as link flaps and the network card switches out of bypass. Inspection resumes after the endpoints reconnect and reestablish link with the device interfaces. The hardware bypass option is **not** supported on nonbypass network modules on ASA with FirePOWER Services on Firepower 8000 Series devices, or SFP transceivers on Firepower 7000 Series.
	inline with optional hardware bypass module, bypass disabled (**Bypass Mode**: **Non-Bypass)**	dropped
7000 and 8000 Series NGIPSv	inline with no hardware bypass module	dropped
	inline in tap mode	egress packet immediately, copy not inspected
	passive	uninterrupted, not inspected
	routed, switched	dropped
ASA FirePOWER	routed or transparent, fail-open (**Permit Traffic**)	passed without inspection (requires at least the minimum supported ASA OS version; otherwise, traffic dropped)
	routed or transparent, fail-close (**Close Traffic**)	dropped

Traffic Behavior When Updating FXOS on Clustered Firepower Threat Defense Devices

Updating FXOS reboots the chassis, which drops traffic in a clustered environment until at least one module comes online.

Traffic Behavior During Configuration Deployment

During the upgrade process, you deploy configurations either twice (standalone devices) or three times (devices managed by the Firepower Management Center). When you deploy, resource demands may result in a small number of packets dropping without inspection. In most cases, the deployment immediately after the upgrade restarts the Snort process. During subsequent deployments, the Snort process restarts only if, before deploying, you modify specific policy or device configurations that always restart the process when deployed.

The following table describes how different devices handle traffic during Snort process restarts.

Table 5 Restart Traffic Effects by Managed Device Model

Device Model	Interface Configuration	Restart Traffic Behavior
Firepower Threat Defense, Firepower Threat Defense Virtual, 7000 and 8000 Series, NGIPSv	inline, **Failsafe** enabled or disabled	passed without inspection A few packets might drop if Failsafe is disabled and Snort is busy but not down
	inline, tap mode	egress packet immediately, copy bypasses Snort
	passive	uninterrupted, not inspected
Firepower Threat Defense, Firepower Threat Defense Virtual	routed, transparent (including EtherChannel, redundant, subinterface)	dropped
7000 and 8000 Series	routed, switched, transparent	dropped
ASA FirePOWER	routed or transparent with fail-open (**Permit Traffic**)	passed without inspection
	routed or transparent with fail-close (**Close Traffic**)	dropped

Audit Logging During the Update

When updating appliances that have a web interface, after the system completes its pre-update tasks and the streamlined update interface page appears, login attempts to the appliance are not reflected in the audit log until the update process is complete and the appliance reboots.

Time and Disk Space Requirements for Updating to Version 6.0.1

The table below provides disk space and time guidelines for the Version 6.0.1 update. Note that when you use the Firepower Management Center to update a managed device, the Firepower Management Center requires additional disk space on its `/Volume` partition.

Caution: Do not restart the update or reboot your appliance at any time during the update process. Cisco provides time estimates as a guide, but actual update times vary depending on the appliance model, deployment, and configuration. Note that the system may appear inactive during the pre-checks portion of the update and after rebooting; this is expected behavior.

The reboot portion of the update includes a database check. If errors are found during the database check, the update requires additional time to complete. System daemons that interact with the database do not run during the database check and repair.

Note: The closer your appliance's current version to the release version (Version 6.0.1), the less time the update takes.

If you encounter issues with the progress of your update, contact Support.

Table 6 Time and Disk Space Requirements

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time
Firepower Management Centers (the MC750, MC1500, MC3500, MC2000, and the MC4000)	18 MB	8959 MB	n/a	66 minutes
64-bit Firepower Management Centers Virtual	MB	MB	n/a	hardware dependent
7000 Series and 8000 Series devices (the 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8380, and the AMP8390)	227 MB	3683 MB	614 MB	30 minutes
Cisco ASA with Firepower Services (the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, and the ASA 5585-X-SSP-60)	54 MB	2966 MB	429 MB	91 minutes
ASA FirePOWER device managed via ASDM (the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, and the ASA 5585-X-SSP-60)	54 MB	2966 MB	429 MB	91 minutes
NGIPSv (virtual managed devices)	196 MB	2090 MB	350 MB	hardware dependent
Cisco ASA with Firepower Threat Defense (the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, and the ASA 5555-X)	1 MB	3685 MB	631 MB	33 minutes
Firepower 9300 Series with Threat Defense	1 MB	3685 MB	631 MB	66 minutes

Firepower Version Requirements for Updating to Version 6.0.1

Appliances must be running the minimum versions specified in the following table in order to update to Version 6.0.1 of the Firepower System. For minimum operating system requirements and information about management platform-managed device compatibility, see Supported Platforms and Compatibility, page 1.

Note: A Firepower Management Center must be running at least Version 6.0.1 if you want to use it to update its managed devices to Version 6.0.1.

Table 7 Platform Support in Version 6.0.1

Platform	Minimum version required to update to Version 6.0.1
Firepower Management Centers (the MC750, MC1500, MC3500, MC2000, and the MC4000)	Version 6.0
64-bit Firepower Management Centers Virtual	Version 6.0
Firepower 7000 Series and 8000 Series (the 7010, 7020, 7030, 7050, 7110, 7115,7120, 7125,8120, 8130, 8140, 8250,8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8380, and the AMP8390)	Version 6.0
Cisco ASA with FirePOWER Services (the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, and the ASA 5516-X, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, and the ASA 5585-X-SSP-60)	Version 6.0
ASA Firepower module managed via ASDM (the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, and the ASA 5585-X-SSP-60)	Version 6.0
NGIPSv (virtual managed devices)	Version 6.0
Cisco ASA with Firepower Threat Defense (the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, and the ASA 5555-X)	Version 6.0
Firepower 4100 Series with Threat Defense (the 4110, 4120, and the 4140)	Version 6.0.1
Firepower 9300 Series with Threat Defense	Version 6.0.1
Firepower Threat Defense Virtual: VMware	Version 6.0

Web Browser and Screen Resolution Compatibility in Version 6.0.1

Note the following to optimize your experience using the web interface.

Web Browser Compatibility

Version 6.0.1 of the web interface for the Firepower System has been tested on the browsers listed in the following table.

Note: The Chrome browser does not cache static content, such as images, CSS, or Javascript, with the system-provided self-signed certificate. This may cause the system to redownload static content when you refresh. To avoid this, add a self-signed certificate to the trust store of the browser/OS or use another web browser.

Note: If you use the Microsoft Internet Explorer 11 browser, you must disable the **Include local directory path when uploading files to server** option in your Internet Explorer settings via **Tools > Internet Options > Security > Custom level**.

Table 8 Supported Web Browsers

Browser	Required Enabled Options and Settings
Chrome 48	JavaScript, cookies
Firefox 44	JavaScript, cookies, Secure Sockets Layer (SSL) v3
Microsoft Internet Explorer 10 and 11	JavaScript, cookies, Secure Sockets Layer (SSL) v3, 128-bit encryption, **Active scripting** security setting, Compatibility View, set **Check for newer versions of stored pages to Automatically**

Note: Many browsers use Transport Layer Security (TLS) v1.3 by default. If you have an active SSL policy and your browser uses TLSv1.3, websites that support TLSv1.3 fail to load As a workaround, configure your managed device to remove extension 43 (TLS 1.3) from ClientHello negotiation. See this software advisory for more information.

Screen Resolution Compatibility

Cisco recommends selecting a screen resolution that is at least 1280 pixels wide. The user interface is compatible with lower resolutions, but a higher resolution optimizes the display.

Integrated Product Compatibility in Version 6.0.1

The required versions for the following integrated products vary by Firepower System version:

- Cisco Identity Services Engine (ISE)
- Cisco AMP Threat Grid
- Cisco Firepower System User Agent

For more information, see the *Firepower System Compatibility Guide*.

Installing the Update

Before you begin the update, you must thoroughly read and understand these release notes, especially Supported Platforms and Compatibility, page 1 and Before You Begin: Important Update and Compatibility Notes, page 11.

Note: To reduce the time to update to Version 6.0.1, install the Version 6.0.1 Pre-Installation Package before you update. For more information, see the *FireSIGHT System Release Notes for Version 6.0.1 Pre-Installation Package*.

Caution: Updates can require large data transfers from the Firepower Management Center to managed devices. Before you begin, make sure your management network has sufficient bandwidth to successfully perform the transfer. See the Troubleshooting Tech Note at https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212043-Guidelines-for-Downloading-Data-from-the.html.

For minimum Firepower System version requirements, see Firepower Version Requirements for Updating to Version 6.0.1, page 15. To update your appliances, see the guidelines and procedures outlined below:

- Updating Firepower Management Centers, page 19
- Updating Managed Devices and ASA Firepower modules, page 21
- Updating Firepower Threat Defense Devices, page 22

Caution: Do not reboot or shut down your appliances during the update until you see the login prompt. The system may appear inactive during the pre-checks portion of the update; this is expected behavior and does not require you to reboot or shut down your appliances.

When to Perform the Update

Because the update process may affect traffic inspection, traffic flow, and link state, Cisco **strongly** recommends you perform the update in a maintenance window or at a time when the interruption will have the least impact on your deployment.

Installation Method

Use the Firepower Management Center's web interface to perform the update. Update the Firepower Management Center first, then use it to update the devices it manages.

Order of Installation

Update your Firepower Management Centers before updating the devices they manage.

Firepower Threat Defense is new for Version 6.0 of the Firepower System. For information about installing Version 6.0.1 a Firepower Threat Defense image on supported ASA models, see the *Cisco Firepower Threat Defense Quick Start Guide*.

Installing the Update on Firepower Management Centers

Updating Firepower Management Center in a high availability pair is not supported in Version 6.0.x or Version 6.0.1.x. In order to update Firepower Management Centers in a high availability environment, you must break the pair and update each Firepower Management Center individually. In order to update to Version 6.0.1, you must break the high availability pair.

Caution: Although the configuration options for Firepower Management Center high availability appear in the Integration page of the user interface, high availability is not supported for Firepower Management Centers in this release. Do not attempt to place Firepower Management Centers into high availability.

Installing the Update on Firepower Threat Defense High Availability Devices

When you install an update on Firepower Threat Defense devices in a high availability pair, the system updates the devices one at a time. When the update starts, the system first applies it to the secondary device, which goes into maintenance mode until any necessary processes restart and the device is processing traffic again. The system then updates the primary device, which follows the same process.

When you update a Cisco ASA with FirePOWER Services high availability pair, apply the update one device at a time, allowing the update to complete before updating the second device.

Installing the Update on Stacked Devices

When you install an update on stacked devices, the system performs the updates simultaneously. Each device resumes normal operation when the update completes. Note that:

- If the primary device completes the update before all of the secondary devices, the stack operates in a limited, mixed-version state until all devices have completed the update.
- If the primary device completes the update after all of the secondary devices, the stack resumes normal operation when the update completes on the primary device.

When you update clustered Firepower Threat Defense devices, the primary device completes the update after all of the secondary devices. You **must** reboot the device cluster before you deploy configuration from the Firepower Management Center.

Caution: Prior to updating a Firepower 9300 Firepower Threat Defense device to Version 6.0.1, you must update the device to FXOS 1.1.4. The device will experience a disruption in traffic during the update. This is expected behavior.

After the Installation

After you perform the update on either the Firepower Management Center or managed devices, you **must** redeploy your configurations. For more information, see the *Firepower Management Center Configuration Guide*.

Caution: When you deploy configurations, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations requires the Snort process to restart, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the managed device handles traffic. For more information, see the Configurations that Restart the Snort Process section of the *Firepower Management Center Configuration Guide*.

There are several additional post-update steps you should take to ensure that your appliances are performing properly. These include:

- verifying that the update succeeded
- making sure that all appliances in your deployment are communicating successfully
- updating to the latest patch for Version 6.0.1, if available, to take advantage of the latest enhancements and security fixes
- optionally, updating your intrusion rules and vulnerability database (VDB) and redeploying your configurations
- making any required configuration changes based on the information in New Features and Functionality, page 7

The next sections include detailed instructions not only on performing the update, but also on completing any post-update steps. Make sure you complete all of the listed tasks.

Updating Firepower Management Centers

Use the procedure in this section to update your Firepower Management Centers, including virtual Firepower Management Centers. For the Version 6.0.1 update, Firepower Management Centers reboot.

Caution: Before you update the Firepower Management Center, redeploy your configurations to any managed devices. Otherwise, the managed device update may fail.

Caution: Do not reboot or shut down your appliances during the update until after you see the login prompt. The system may appear inactive during the pre-checks portion of the update; this is expected behavior and does not require you to reboot or shut down your appliances.

Note: Updating a Firepower Management Center to Version 6.0.1 removes existing uninstallers from the appliance.

To update a Firepower Management Center:

Step 1 Read these release notes and complete any required pre-update tasks.

Step 2 Download the update from the Support site:

- for Firepower Management Centers and Firepower Management Centers Virtual:

```
Sourcefire_3D_Defense_Center_S3_Upgrade-6.0.1-1222.sh
```

Note: Download the update directly from the Support site. If you transfer an update file by email, it may become corrupted.

Step 3 Upload the update to the Firepower Management Center by selecting **System > Updates**, then clicking **Upload Update** on the **Product Updates** tab. Browse to the update and click **Upload**.

The update is uploaded to the Firepower Management Center. The web interface shows the type of update you uploaded, its version number, and the date and time it was generated.

Step 4 Make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Step 5 Click the System Status icon, then click the Tasks tab and make sure that there are no tasks in progress.

You **must** wait until any long-running tasks are complete before you begin the update. After the system update completes, to reduce clutter, remove the messages for these tasks from the Message Center.

Step 6 Select **System > Updates.**

The Product Updates tab appears.

Step 7 Click the install icon next to the update you uploaded.

The Install Update page appears.

Step 8 Select the Firepower Management Center and click **Install**. Confirm that you want to install the update and reboot the Firepower Management Center.

The update process begins. To view the task status, click the System Status icon, then click on the Tasks tab. However, after the Firepower Management Center completes its necessary pre-update checks, you are logged out. When you log back in, the Upgrade Status page appears. The Upgrade Status page displays a progress bar and provides details about the script currently running.

If the update fails for any reason, the page displays an error message indicating the time and date of the failure, which script was running when the update failed, and instructions on how to contact Support. Do **not** restart the update.

Caution: If you encounter any other issue with the update (for example, if a manual refresh of the Update Status page shows no progress for several minutes), do not restart the update. Instead, contact Support.

When the update completes, the Firepower Management Center displays a success message and reboots.

Step 9 After the update finishes, clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.

Step 10 Log into the Firepower Management Center.

Step 11 Review and accept the End User License Agreement (EULA). Note that you are logged out of the appliance if you do not accept the EULA.

Step 12 Select **Help > About** and confirm that the software version is listed correctly: Version 6.0.1. Also note the versions of the intrusion rule update and VDB on the Firepower Management Center; you will need this information later.

Step 13 Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Step 14 If the rule update available on the Support site is newer than the rules on your Firepower Management Center, import the newer rules. Do not auto-apply the imported rules at this time.

For information on rule updates, see the *Firepower Management Center Configuration Guide*.

Step 15 If the VDB available on the Support site is newer than the VDB on your Firepower Management Center, install the latest VDB.

Installing a VDB update causes a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the *Firepower Management Center Configuration Guide*.

Step 16 Redeploy your configurations to all managed devices.

Deployment may cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the *Firepower Management Center Configuration Guide*.

Step 17 If a patch for Version 6.0.1 is available on the Support site, apply the latest patch as described in the *Firepower System Release Notes* for that version.

Caution: When you deploy configurations, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations requires the Snort process to restart, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the managed device handles traffic. For more information, see the Configurations that Restart the Snort Process section of the *Firepower Management Center Configuration Guide*.

You **must** update to the latest patch to take advantage of the latest enhancements and security fixes.

Caution: Although the configuration options for Firepower Management Center high availability appear in the Integration page of the user interface, high availability is not supported for Firepower Management Centers in Version 6.0.1. Do not attempt to place Firepower Management Centers into high availability.

Updating Managed Devices and ASA Firepower modules

After you update your Firepower Management Centers to Version 6.0.1, use them to update the devices they manage.

You must use a Firepower Management Center running Version 6.0 to update any managed device that does not have its own web interface. For ASA Firepower modules running on the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, or ASA 5516-X, you can update the module using the Firepower Management Center or connect to the ASA device and update the ASA Firepower module using local management via ASDM. For more information see the *Cisco ASA with FirePOWER Services Local Management Release Notes*.

Updating managed devices is a two-step process. First, download the update from the Support site and upload it to the managing Firepower Management Center. Next, install the software. You can update multiple devices at once, but only if they use the same update file.

When you update clustered Cisco ASA with FirePOWER Services, apply the update one device at a time, allowing the update to complete before updating the second device.

For the Version 6.0.1 update, all devices reboot. 7000 Series and 8000 Series devices do **not** perform traffic inspection, switching, routing, NAT, VPN, or related functions during the update and devices running Firepower Threat Defense do **not** perform VPN functions. Depending on how your devices are configured and deployed, the update process may also affect traffic flow and link state. For more information, see Traffic Flow and Inspection During the Update, page 12.

Firepower Threat Defense is new for the Version 6.0 Firepower System. You can reimage your Cisco ASA with FirePOWER Services to use Firepower Threat Defense, or you can reimage Cisco ASA devices with Firepower Threat Defense to a supported ASA version. For information about installing a Version 6.0.1 Firepower Threat Defense image on supported ASA models, see the *Cisco Firepower Threat Defense Quick Start Guide*.

Caution: Before you update a managed device, use its managing Firepower Management Center to redeploy your configuration to the managed device. Otherwise, the managed device update may fail.

Caution: Installing an update and deploying configurations can interrupt traffic inspection due to Snort restarts and system restarts. How these interruptions affect traffic depends on how the managed device handles traffic. For more information, see Traffic Flow and Inspection During the Update, page 12.

Caution: Do not reboot or shut down your appliances during the update until after you see the login prompt. The system may appear inactive during the pre-checks portion of the update; this is expected behavior and does not require you to reboot or shut down your appliances.

To update managed devices and ASA Firepower modules:

Step 1 Read these release notes and complete any required pre-update tasks.

For more information, see Before You Begin: Important Update and Compatibility Notes, page 11.

Step 2 Update the software on the devices' managing Firepower Management Center; see Updating Firepower Management Centers, page 19.

Step 3 Download the update from the Support site:

- for 7000 Series and 8000 Series managed devices:

  `Sourcefire_3D_Device_S3_Patch-6.0.1-29.sh`

- for virtual managed devices:

  `Sourcefire_3D_Device_Virtual64_VMware_Patch-6.0.1-29.sh`

- for ASA Firepower modules:

  `Cisco_Network_Sensor_Patch-6.0.1-29.sh`

Note: Download the update directly from the Support site. If you transfer an update file by email, it may become corrupted.

Step 4 Upload the update to the Firepower Management Center by selecting **System > Updates**, then clicking **Upload Update** on the Product Updates tab. Browse to the update and click **Upload**.

The update is uploaded to the Firepower Management Center. The web interface shows the type of update you uploaded, its version number, and the date and time it was generated.

Step 5 Make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Step 6 Click the install icon next to the update you are installing.

The Install Update page appears.

Step 7 Select the devices where you want to install the update.

If you are updating a stacked pair, selecting one member of the pair automatically selects the other. You must update members of a stacked pair together.

Step 8 Click **Install**. Confirm that you want to install the update and reboot the devices.

Step 9 The update process begins. Monitor the update's progress in the Firepower Management Center by clicking the System Status icon, then clicking the Tasks tab.

Note that managed devices may reboot twice during the update; this is expected behavior.

Caution: If you encounter issues with the update (for example, if the Message Center indicates that the update has failed, or shows no progress on the update task for several minutes), do not restart the update. Instead, contact Support.

Step 10 Select **Devices > Device Management** and confirm that the devices you updated have the correct software version: Version 6.0.1.

Step 11 Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Step 12 Redeploy your configurations to all managed devices.

Deployment may cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the *Firepower Management Center User Guide*.

Step 13 If a patch for Version 6.0.1 is available on the Support site, apply the latest patch as described in the release notes for that version.

Caution: When you deploy configurations, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations requires the Snort process to restart, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the managed device handles traffic. For more information, see the Configurations that Restart the Snort Process section of the *Firepower Management Center Configuration Guide*.

Updating Firepower Threat Defense Devices

After you update your Firepower Management Centers to Version 6.0.1, use them to update the devices they manage. You can update ASA devices and Firepower 9300 Security Appliances running the Firepower Threat Defense preview version 6.0.0 to Version 6.0.1. This procedure documents update of Firepower Threat Defense running on at least Version 6.0.0. A Firepower Management Center must be running at least Version 6.0.1 to update Firepower Threat Defense devices to Version 6.0.1. Because they do not have a web interface, you must use the Firepower Management Center to update these devices.

Updating managed devices is a two-step process. First, download the update from the support site and upload it to the managing Firepower Management Centerr. Next, install the software. You can update multiple devices at once, but only if they use the same update file.

Caution: Before you update a managed device, use its managing Firepower Management Center to redeploy policies to the managed device. Otherwise, the managed device update may fail

Caution: Do not reboot or shut down your appliances during the update until after you see the login prompt.

To update your appliances, see the guidelines and procedures outlined below:

Step 1 Read these release notes and complete any required pre-update tasks.

For more information, see Before You Begin: Important Update and Compatibility Notes, page 11.

Step 2 Update the software on the devices' managing Firepower Management Center; see Updating Firepower Management Centers, page 19.

Step 3 If you are updating a Firepower 9300 Security Appliance, update the operating system to FXOS 1.1.4 and restart the system; for more information see the *Cisco FXOS Firepower Chassis Manager Configuration Guide*.

Caution: Updating the Firepower 9300 Security Appliance to FXOS 1.1.4 causes a disruption in traffic. This is expected.

You **must** update the ROMMON image on ASA Firepower modules to Version 1.1.8 prior to updating to Version 6.0.1. For more information about updating the ROMMON image, see *Cisco ASA Series General Operations CLI Configuration Guide*.

Step 4 Download the update from the Support site:

- for Firepower Threat Defense running on the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, or on VMware:

  `Cisco_FTD_Upgrade-6.0.1-29.sh`

- for Firepower Threat Defense running on the Firepower 9300 Security appliance:

  `6.0.1-29.SPA.csp`

- for Firepower Threat Defense Virtual: VMware

  `Cisco_FTD_Upgrade-6.0.1-29.`

Step 5 Upload the update to the Firepower Management Center by selecting **System > Updates**, then clicking Upload Update on the Product Updates tab. Browse to the update and click **Upload**.

The update is uploaded to the Firepower Management Center. The web interface shows the type of update you uploaded, its version number, and the date and time it was generated. The page also indicates whether a reboot is required as part of the update.

Step 6 Make sure the appliances in your deployment are successfully communicating that there are no issues reported by the health monitor.

Step 7 Click the install icon next to the update you are installing.

Step 8 Select the devices where you want to install the updated.

Step 9 click **Install**. Confirm that you want to install the update and reboot the devices.

Step 10 The update process begins. You can monitor the update's progress on the Tasks tab of the Message Center.

Note: Devices may reboot twice during the update; this is expected behavior.

Caution: If you encounter issues with the update (if messages in the Tasks tab of the Message Center show no progress for several minutes or indicate that the update has failed), do not restart the update. Instead, contact Support.

Step 11 Select **Devices > Device Management** and confirm that the devices you updated have the correct software version: 6.0.1.

Step 12 Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Step 13 Redeploy policies to all managed devices.

Click the **Deploy** button and select all available devices, then click **Deploy**.

Resolved Issues

You can view defects resolved in this release using the Cisco Bug Search Tool (https://tools.cisco.com/bugsearch/). A Cisco account is required.

The following issues are resolved in Version 6.0.1:

- Security Issue Addressed multiple vulnerability issues that generated denial of service in NTP, and other third parties as described in CVE-2015-7704, CVE-2015-7705, CVE-2015-7853, and CVE-2015-7855.(
- Security Issue Addressed multiple arbitrary script injection vulnerabilities allowing unauthenticated, remote attackers to exploit or overwrite functionality as described in CVE-2015-7703.
- Security Issue Addressed a vulnerability in the third party product NTP as described in CVE-2015-7852.
- Security Issue Addressed an arbitrary HTTP header injection vulnerability allowing unauthenticated, remote attackers to exploit managed devices as described in CVE-2016-134.
- Resolved an issue where, if you configured Open Shortest Path First (OSPF) in the Dynamic Routing tab of the Virtual router page (**Devices > Devices Management > Virtual routers > Dynamic Routing**) and added an **Area**, then changed the value of the **Cost** column and deployed changes, the system did not update the OSPF. (CSCus31735)
- Improved the stability of Snort functionality. (CSCut75876)
- Resolved an issue where you could not manually set the time zone on an ASA Firepower module managed by ASDM. (CSCuu70250)
- Resolved an issue where, if you attempted to update the system with less than the required amount of free space, the update failed and the system incorrectly appeared to have a negative amount of space available. (CSCuv43019)
- Resolved an issue where, in some cases, registered devices generated extraneous logs and the system experienced issues. (CSCuw84304)
- Resolved an issue where, if you registered an ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, or ASA 5585-X-SSP-60 device running Firepower services to a Firepower Management Center and enabled **Clientless VPN tunnel group**, then deployed an access control policy with the default action set to **Allow** all traffic, the system incorrectly dropped packets. (CSCuw38561)
- Improved inspection of encrypted FTP traffic using recently updated FTP standards. (CSCux02171)
- Resolved an issue where in some cases pinholes were not created for RTP connections established by calls using the SIP protocol, which prevented the VOIP channel creation for the SIP call. (CSCux03758)
- Improved HTTP traffic processing and reduced the chance of dropped packets when processing HTTP POST events that are large. (CSCux11773)
- Resolved an issue where, if you reboot a managed NGIPSv device and added multiple vmxnet3 interfaces, the system incorrectly added the interfaces causing pre-existing interfaces to experience issues. (CSCux15018)
- Resolved an issue where disabling interface `eth0` caused system issues. (CSCux22564)
- Improved Cisco Security Manager (CSM) troubleshooting. (CSCux30600)
- Resolved an issue where, if you created an access control policy referencing an SSL policy containing a network object with multiple entries on a managed Firepower appliance running Version 5.4 or later and you updated the system to Version 6.0, policy apply failed. (CSCux31618)
- Resolved an issue where, if an LDAP group containing the following special characters is explicitly included or excluded from the LDAP download, the system experienced issues and did not download any group or user: (**{**), (**}**), and (**#**). (CSCux46525)
- Improved reliability of pre-processing of DCERPC2 traffic in low memory conditions. (CSCux48253)
- Resolved an issue where, if you deployed a file policy with the default action set to **Malware Block** and the system detected SMB traffic, the system experienced issues. (CSCux49653)
- Resolved an issue where the system used an invalid format for the default name of a Distinguished Name object. (CSCux54184)

- Resolved an issue where Teredo traffic matching an IP any any pass intrusion rule or an alert intrusion rule caused dropped traffic or system issues. (CSCux55780)
- Resolved an issue where, if you edited and deployed an intrusion policy that was created in Version 5.4 or earlier, intrusion layers may have corrupted. (CSCux57697)
- Improved the stability of SSL traffic inspection. (CSCux59557)
- Resolved an issue where, if you deployed an intrusion policy and enabled Sensitive Data Detection, the system did not consistently mask content in traffic containing sensitive data. (CSCux61562)
- Improved packet reassembly for HTTP traffic. (CSCux61630)
- Resolved an issue where, if you deployed an SSL policy configured to **Decrypt -Resign** and attempted to download a large file on a high speed LAN, the system experienced issues. (CSCux66909)
- Improved the stability of using IPv6 IP with Cisco redundancy protocol (SFRP). (CSCux67113)
- If you update an ASA with FirePOWER services to Version 6.0.0.1 and switch the device to an ASA Firepower module managed via ASDM, the system now automatically generates a default access control policy to be deployed. (CSCux69362)
- Resolved an issue where, if you deployed an SSL policy and enabled SSL decryption, the system experienced a disruption in traffic after a few hours of decrypting SSL traffic. (CSCux75036)
- Improved HTTP inspection of gzip compressed data when there is no Content-Length header present in the HTTP Response. (CSCux76518)
- Resolved an issue where, if you updated an ASA Firepower module managed by ASDM to Version 6.0.0.1 and switched the device to an ASA with FirePOWER Services device, the Access Control Policy page (**Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**) did not generate the default access control policy. (CSCux76581)
- Improved the fail-to-wire function on Firepower 7110, 7115, 7120, 7125, and 7150 devices. (CSCux84120)
- Resolved an issue where, if a device running Firepower Threat Defense remained registered to a Firepower Management Center for ten days or more, the Firepower Management Center generated errors if you attempted to register a new device, update the Firepower Management Center, create a backup, or edit a domain and you could not perform those actions. (CSCux89875)
- Resolved an issue where, if you deployed a file policy and added a SHA value to the global blacklist or global whitelist on an ASA Firepower device managed by ASDM, the system did not update the blacklist or whitelist to include the SHA value and did not mark the file policy as out-of-date. (CSCux91872)
- Resolved an issue where, if you deployed an access control policy containing an SSL rule, the system eventually dropped the majority of incoming traffic and caused a network outage. (CSCux95913)
- Resolved an issue where, if you deployed a network discovery policy with **Applications** disabled and a network analysis policy with the HTTP Inspect preprocessor enabled or a file policy, the system ran out of memory and stopped detecting traffic. (CSCux96457)
- Resolved an issue where, if a 7000 Series or 8000 Series in a high availability pair experienced a failover, the system did not correctly recover shared configurations, and the system experienced issues. (CSCuy20064)
- Improved stability of network mapping while applying domain configuration changes. (CSCuy30050)
- Resolved an issue where, if you created a 7000 Series or 8000 Series high availability pair in a leaf domain and broke the high availability pair in a global domain, the system erroneously generated a `Load container -Invalid domain permission` error even though the high availability successfully broke. (CSCuy30473)
- Resolved an issue where, if you deployed an access control policy referencing at least one intrusion rule in a leaf domain and then viewed the Packets view of the Intrusion Events page (**Analysis > Intrusion > Intrusion Events**) in the global domain, the system did not display packet information from the leaf domain. (CSCuy30532)
- Resolved an issue where, if you deployed an SSL policy to registered NGFW device experiencing light traffic load, the system delayed packet delivery for ten seconds or more. (CSCuy52349)
- Resolved an issue where, if you created a variable set containing a group of multiple network objects the system incorrectly saved the variable set's default value as `any`. (CSCuy60748)

Version 6.0

The following issues were resolved in Version 6.0:

- Security Issue Addressed a cross-site request forgery (CSRF) vulnerability.
- Security Issue Addressed a vulnerability that allowed an authenticated user can access system files using path traversal.
- Security Issue Addressed multiple cross-site scripting (XSS) vulnerabilities, including those described in CVE-2015-0737, CVE-2015-4270, and CVE-2015-6353.
- Security Issue Addressed multiple cross-site scripting (XSS) and arbitrary HTML injection vulnerabilities including those described in CVE-2015-0707.
- Security Issue Addressed multiple vulnerability issues in MYSQL, DNS, NTP, and OpenSSL as described in CVE-2010-3614, CVE-2014-3569, CVE-2014-3570, CVE-2014-3572, CVE-2014-6568, CVE-2014-9293, CVE-2014-9294, CVE-2014-9295, CVE-2014-9296, CVE-2014-9297, CVE-2014-9298, CVE-2015-0205, CVE-2015-0287, CVE-2015-0292, CVE-2015-0374, CVE-2015-0381, CVE-2015-0382, CVE-2015-0385, CVE-2015-0391, CVE-2015-0409, CVE-2015-0411, CVE-2015-0432, CVE-2015-0498, CVE-2015-0505, CVE-2015-0506, CVE-2015-0507, CVE-2015-0511, CVE-2015-1798, CVE-2015-1799, CVE-2015-1499, CVE-2015-2566, CVE-2015-2567, CVE-2015-3405, CVE-2015-3676.
- Security Issue Addressed multiple vulnerability issues that generated denial of service in MYSQL, Linux, GNU C Library, NTP, XML, OpenSSL, and other third parties as described in CVE-2009-0696, CVE-2011-1155, CVE-2012-0876, CVE-2012-2807, CVE-2012-287, CVE-2012-3509, CVE-2012-3400, CVE-2012-3480, CVE-2012-5134, CVE-2013-0242, CVE-2013-1914, CVE-2013-4332, CVE-2013-4458, CVE-2014-3512, CVE-2014-3571, CVE-2014-3660, CVE-2014-6040, CVE-2014-8502, CVE-2015-0206, CVE-2015-0286, CVE-2015-0288, CVE-2015-0293, CVE-2015-1473, CVE-2015-1781, CVE-2015-1819.
- Security Issue Addressed multiple arbitrary script injection vulnerabilities allowing unauthenticated, remote attackers to exploit or overwrite functionality as described in CVE-2008-3075, CVE-2008-4101, CVE-2010-2252, CVE-2010-4494, CVE-2010-4651, CVE-2011-2716, CVE-2011-3102, CVE-2014-047, CVE-2014-4877, CVE-2014-5119, CVE-2014-7817, CVE-2015-1472, CVE-2015-6307.
- Security Issue Addressed multiple vulnerabilities in HTTP connection handling that allowed users to be redirected to malicious websites as described in CVE-2012-1033 and CVE-2015-0706.
- Security Issue Addressed multiple vulnerabilities that allowed unauthenticated, remote attacker to disclose sensitive information on an affected system, including those described in CVE-2011-1098 and CVE-2015-3153.
- Security Issue Addressed multiple vulnerabilities in SSLv3 that allowed external attacks on client connections, as described in CVE-2014-3556.
- Security Issue Addressed multiple parameter manipulation and misconfiguration vulnerabilities, including those described in CVE-2009-0025, CVE-2009-4022, and CVE-2015-0773.
- Security Issue Resolved multiple vulnerabilities where managed devices experienced microengine failure when processing traffic, including those described in CVE-2015-6307.
- Resolved an issue where, if the device did not process sufficient traffic, the system failed to generate complete performance graphs. (108348/CSCze87001)
- Resolved an issue where the intrusion performance graph incorrectly reported the minimum packets received instead of the actual number of packets received. (124331/CSCze87003)
- Resolved an issue where deploying a policy with a policy identification number greater than `4096` failed. (134385/CSCze89030)
- Resolved an issue which could have artificially limited the number of active dynamic NAT translations. (134561/CSCze87078)
- Resolved an issue where, in some cases, the front panel LCD informational screen of Firepower 7000 Series and 8000 Series devices incorrectly displayed some software errors as hardware errors. (140386/CSCze91939)
- Resolved an issue where the system did not display the number of failed login attempts. (140400/CSCze87152)
- Improved data pruning. (141894/ CSCze92576)

- Improved link state propagation responsiveness for Firepower 7000 Series and 8000 Series devices (143860/CSCze87386)
- Resolved an issue where, if you disabled an access control rule using an intrusion policy or variable set not used in any other rule and attempted to deploy the policy, deployment failed. (143872/CSCze87308)
- Improved URL filtering. (144198/CSCze94590, 144199/CSCze94758, 144685/CSCze94805)
- Resolved an issue where, if updating failed and you attempted to update again, some drives did not mount correctly during install. (144553/CSCze95696)
- Improved reporting. (145102/CSCze95656)
- Resolved an issue where the Discovery Statistics page did not include any events in the following rows of the statistics summary: **Total Events**, **Total Events Last Hour**, or **Total Events Last Day**. (145153/CSCze95751)
- Improved troubleshooting for Firepower 7000 Series and 8000 Series devices. (145187/CSCze95510)
- Resolved an issue where removing the URL Filtering license from your system caused a disruption in cloud connectivity. (144578/CSCze95183)
- Corrected the calculation used by the memory usage health monitor to prevent false alerts. (144593/CSCze94840)
- Resolved an issue where the passive interfaces on Firepower 7000 Series devices reported incorrect egress security zones and interfaces. (144624/CSCze95206)
- Resolved an issue where, if you edited the interface security zones on the Object Management page, the stacked device configuration appeared to be up-to-date when it wasn't. (144626/CSCze94847)
- Resolved an issue where, if you deployed to a cluster or device stack of Firepower 7000 Series or 8000 Series devices, the system only deployed to the primary device if the clustered or stacked devices contained out-of-date policies prior to latest policy apply. (144646/CSCze95167)
- Resolved an issue where, if you created an HTML report, the web browser incorrectly displayed the report as binary data.(144737/CSCze95180, 144738/CSCze95205)
- Resolved an issue where decrypted SSL sessions displayed URLs in connection logs as http:// instead of https://. (144785/CSCze95781)
- Resolved an issue where, if you created a custom network variable named identically to a default variable but with different capitalization, the system incorrectly assumed the custom variable and the default variable were the same and prevented you from deleting the custom variable. (44788/CSCze96160)
- Resolved an issue where the system treated DNS traffic as OpenVPN, QQ, and Viber traffic. (144789/CSCze96154)
- Resolved an issue where if you imported a policy that referenced a shared layer, importing the policy failed. (144946/CSCze96151)
- Improved disk space utilization. (145012/CSCze95309)
- Improved reliability of hardware acceleration in Firepower 7000 Series and 8000 Series devices. (145035/CSCze95433, 145509/CSCze95994, CSCus68624, CSCut53335, CSCut80043)
- Resolved an issue where, if you edited a local rule on the intrusion rule editor when viewing rule documentation, the system displayed the current local rule configuration for already-generated event data instead of the rule configuration that triggered it. (145118/CSCze95346)
- Resolved an issue where, if you generated an intrusion even performance graph with **Last Hour** set as the time range, the system incorrectly generated a blank graph. (145237/CSCze95774)
- Resolved an issue where, if you enabled remote storage and created a scheduled email alert response on your Firepower Management Center, the scheduled email alert disabled remote storage and remote storage backups failed. (145288/CSCze95993)
- Resolved an issue where, if you attempted to view the first or last event of an Indication of Compromise (IoC), the system did not locate the event. (145486/CSCze95786)

- Resolved an issue where the 40GB fiber NetMod traffic statistics incorrectly logged traffic on the wrong 40GB port. (145515/CSCze95830)
- Resolved an issue where access control rules containing web application conditions did not match against traffic if users on your network entered a URL into the address bar that was not all lowercase. (CSCur37364)
- Resolved an issue where the file trajectory page failed to load due to invalid subtypes. (CSCur38623)
- Resolved an issue where, in some cases, you were not able to retrieve URL category or URL reputation information. (CSCur38971)
- Resolved an issue where, if you did not deactivate a traffic profile before deleting it, the deleted profile continued to use resources when it should not. (CSCur48345)
- Resolved an issue where, if you created a custom workflow and attempted to open the packet view of an intrusion event, the system opened the incorrect intrusion event in the packet view. (CSCur48743)
- Resolved an issue where, in some cases, you could not edit your access control policy and the system generated an `Unknown Error (9999): Couldn't get a lock on /var/tmp/.ac_lock` error message. (CSCur55338)
- Resolved an issue where, if you created a scheduled task to install a new version of the vulnerability database (VDB) on a Firepower Management Center already running that version of the VDB, the system reinstalled the VDB and switched from active mode to standby mode every time the task was scheduled. (CSCur59252)
- Resolved an issue where, if you created a correlation rule to trigger when an intrusion event or connection event occurs and the condition matches an ingress security zone, egress security zone, ingress interfaces, or egress interface as the condition, the system did not recognize the rule and failed to generate events for traffic matching the rule. (CSCur59840)
- Resolved an issue on Firepower 7000 Series and 8000 Series managed devices where the system lost inline connectivity for up to 25 seconds on bypass-enabled inline sets during device reboot. (CSCur64678)
- You can now disable session termination logging to decrease disk space requirements. (CSCur73008)
- Resolved an issue where the system did not display the associated hosts if you expanded a vulnerability based on a client application from the vulnerabilities tab of the Network Map. (CSCur86191)
- Resolved an issue where, if you configured a routed interface on clustered Firepower 7000 Series or 8000 Series managed devices to both a private IP address and a Cisco Redundancy Protocol (SFRP) IP address, the system did not recognize which IP address was the primary address and did not establish an Open Shortest Path First (OSPF) connection. (CSCur86355)
- Resolved an issue where, if you changed the selected time zone in the Time Zone Preference tab on the User Preferences page, the system did not include daylight savings time. (CSCur92028)
- Resolved an issue where the system did not generate complete troubleshoot files if the system contained a large database. (CSCur97450)
- Resolved an issue where, in some cases, the host did not always display the block page if one of your access control rule actions was set to **Block** or **Interactive Block**. (CSCus06868)
- Resolved an issue where the system incorrectly duplicated the number of registered targets on the Intrusion Policy page. (CSCus08840)
- Resolved an issue where the system occasionally experienced latency during Snort restart. (CSCus11068)
- Resolved an issue where, an ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, or ASA 5555-X device configured in monitor-only mode experienced a fail over if the device processed a high amount of traffic. (CSCus15229)
- Resolved an issue where the system did not support generating multiple report types when using Windows File Sharing (SMB) due to unsupported characters in the report name. (CSCus21871)
- Resolved an issue where, if you configured a domain name without a DNS entry, the web interface page did not load. (CSCus28155, CSCut89714)
- Resolved an issue where importing intrusion rules failed if you edited an intrusion policy. (CSCus29526)
- Resolved an issue where, if you created an SSL policy with the default actions set to **Do Not Decrypt** and attempted to establish a session, the system erroneously reported the session was blocked when it was not. (CSCus41127)

- Resolved an issue where, if you added a Cisco IOS remediation to your Cisco IOS Null Route instance and entered your password to log into the router, the device did not accept the password and remediation failed. (CSCus45769)
- Improved the optimization of certain event workflows. (CSCus52203)
- Resolved an issue where, if the intrusion policy had a sufficiently complex configuration, the system truncated the configuration and intrusion policy deployment failed. (CSCus53911)
- Improved memory utilization. (CSCus59008, CSCuu38535, CSCuu81679)
- Resolved an issue where, if you created an access control rule referencing a file policy with a **Block Malware** rule positioned after an access control rule containing a web application condition, the system did not identify malware files. (CSCus64393, CSCus6452)
- Resolved an issue where the system generated an `Internal Server Error` message if the password for your registered ASA Firepower module included an unsupported character. (CSCus68604)
- Resolved an issue where, if you configured both malware blocking and SSL decryption, you could not download files via HTTPS even if the files did not contain malware. (CSCus72505)
- Improved communication between Firepower Management Centers and managed devices. (CSCus79643)
- You can now deploy an access control policy containing both SSL policies and URL category conditions on a Firepower Management Center with a registered Firepower 7030 device. (CSCut02823)
- Resolved an issue where the system experienced latency when you deleted hosts from the network map. (CSCut02913)
- Improved pruning for correlation event tables. (CSCut02984)
- Resolved an issue where, if you created a file policy with Spero analysis and file capture enabled, the system did not capture files detected in incoming traffic. (CSCut06837)
- Resolved an issue where, if you restored a backup archive located on a Windows network file server (NFS), backup restoration failed. (CSCut08317)
- Resolved an issue where, if you deployed an access control policy referencing an SSL policy to a managed device with **Inspect Local Router Traffic** enabled, the system generated errors and experienced issues. (CSCut12631)
- Resolved an issue where deploying to a cluster of devices (in Version 6.0, known as high availability) caused the system to fail over when it should not. (CSCut12919)
- Resolved an issue where, if you created an access control rule configured to send connection events to an external syslog server and the rule matched an excessive amount of traffic, the managed device stopped sending events to the external syslog server. (CSCut14629)
- Resolved an issue where, if your intrusion policy layers shared identical names and you performed a system update, the system experienced issues. (CSCut16772)
- Improved network mapping generation when processing historical email and eStreamer events. (CSCut23688)
- Resolved an issue where, if you edited an access control rule with multiple URL category conditions and attempted to remove one of the conditions, the system removed only the first category condition listed. (CSCut25082)
- Resolved an issue where, in some cases, the Firepower Management Center experienced system issues and failed to load access control rules. (CSCut30047)
- Resolved an issue where, if you created a passive zone on a Firepower 8000 Series device and performed the `show fastpath-rules` CLI command, the system reported intrusion rules as inactive. (CSCut32479)
- Improved the reliability of backup and restore. (CSCut34456)
- The system generates a `Having Inspect traffic during policy apply disabled may cause network disruptions until deployment completes` warning if you deploy without enabling **Inpsect traffic during policy apply**. (CSCut36078)
- Resolved an issue where, if you created a file policy configured to **Inspect Archives**, the system experienced issues and stopped processing traffic. (CSCut39253, CSCuu14892)

- Resolved an issue where, if you selected one or more cells of the Original Client IP column in the intrusion events table view to review or copy, the system generated an error and did not display the rows you selected. (CSCut41458)
- Resolved an issue where the system experienced latency and did not match traffic if you created an access control rule targeting users in an LDAP group that contains a large number of access-controlled users. (CSCut56233)
- Resolved an issue where, if you created and edited a search for generated events, then canceled it before the search started, the system redirected you to the events page related to the search with the incorrect search name. (CSCut63265)
- Improved disk manager functionality. (CSCut65740)
- Resolved an issue where the system experienced issues if the last entry in the map list was a duplicate. (CSCut65738)
- Resolved an issue where importing intrusion rule updates caused system issues. (CSCut65772)
- Resolved an issue where, in some cases, the system dropped database communication and experienced errors. (CSCut71816)
- Resolved an issue where, in some cases, deploying on a Firepower Management Center with registered Firepower 7000 Series and 8000 Series devices in a high-availability pair caused a fail over. (CSCut72278)
- Improved health alert notifications for Cloud Lookup failures. (CSCut77594)
- Resolved an issue where, if your system experienced two sequential failures, the system was placed into bypass mode even if you did not enable bypass mode. (CSCut80892)
- Resolved an issue where the message column of the Retrospective Malware Events table view did not include the old disposition or the new disposition values of a retrospective malware event. (CSCut83512)
- Resolved an issue where, if you restarted your ASA 5585-X device with a large number of subinterfaces configured without also restarting the SFR5585-X service card, the SFR5585-X service card appeared to fail. (CSCut89619)
- Resolved an issue where using the `show managers` CLI command on a device registered to a system with multiple interfaces configured caused the system displayed the incorrect IP address. (CSCut95947)
- Resolved an issue where, in some cases, update failure did not get caught in time. (CSCuu01055)
- Resolved an issue where, if you experienced system issues, the cloud continuously checked for a new update. (CSCuu04844)
- Resolved an issue where, if you created an access control policy with a URL category condition and the network map failed to load a complete database, the system experienced issues. (CSCuu06714)
- Resolved an issue where the vulnerability database (VDB) install took an unexpectedly long time. (CSCuu06786)
- Resolved an issue where, in some cases, your Firepower Management Center stopped receiving health events from a registered device. (CSCuu18450)
- Resolved an issue where, if you created an access control policy configured with a **Block** or **Block with Reset** action on Cisco ASA Firepower module running on a Firepower Threat Defense, the client did not always display the block page when it should. (CSCuu23884)
- Resolved an issue where the system experienced latency if you created a link aggregation group (LAG) on a Firepower 7000 Series or 8000 Series device when connected to a Cisco Nexus 7000 switch. (CSCuu31626)
- Resolved an issue where, if you changed your system's time zone to a UTC+ zone and added a correlation rule with at least one inactive period to a correlation policy, activating the correlation rule failed. (CSCuu37600)
- Resolved an issue where you experienced connectivity issues if you created a routed interface on your clustered Firepower 7000 Series or 8000 Series device (known as high availability in Version 6.0). (CSCuu37668)
- Resolved an issue where the Cisco Redundancy Protocol (SFRP) router advertisement value appeared to be configurable when you added or edited a routed IP address when it was not. (CSCuu37687)
- Resolved an issue where, if you enabled two or more management interfaces and web client lost connectivity to one of the interfaces, the system defaulted to an incorrect gateway IP address and you could not access the interface. (CSCuu44020)
- Resolved an issue where, if you created an access control policy with a geolocation condition, traffic that should have matched the condition did not. (CSCuu48800)

- Improved network map generation. (CSCuu53215, CSCuu94784, CSCuv72386, CSCuw06359)
- Improved load time for access control rules with manual URL conditions referenced in an access control policy. (CSCuu55853)
- Resolved an issue where ASA Firepower modules (ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, and ASA 5516-X) running the minimum ASA version 9.3.2.2 or later did not enforce the mpf-policy-map-class mode. (CSCuu68273)
- Resolved an issue where creating a search for an intrusion event with an original client IP using a negated subnet IP address caused the system to incorrectly exclude intrusion events with no original client IP. (CSCuu68438)
- Resolved an issue where, in rare cases, the system appeared unstable and did not recover from a reboot. (CSCuu93154)
- Resolved an issue where a drive failure on some DC4000 appliances caused RAID controller failure and data loss. (CSCuu93159)
- Improved eStreamer performance. (CSCuu94902)
- Resolved an issue where the system did not display the correct number of bytes in the Top Web Applications Seen and Top Client Applications Seen widgets on the Summary Dashboard if you viewed high-volume media such as video streaming on your web browser. (CSCuu97036)
- Resolved an issue where, if you deployed an SSL policy set to **Decrypt-Resign** on a managed device, the decrypted traffic that egressed from one interface set switched or routed so the traffic ingressed into a different interface set on the same managed device and the system experienced a disruption in SSL traffic. (CSCuu97712)
- Resolved an issue where the **Send email** check box on the Report Templates tab of the Reporting page did not stay selected and you stopped receiving reports via email if you generated a report, navigated away from the Report Templates tab, and then generated another report. (CSCuu97750, CSCuu41580, CSCuv43116)
- Resolved an issue where clicking **Continue** on interactive block web page did not always redirect you to the blocked web page. (CSCuu97934, CSCuu97946)
- Resolved an issue where, in some cases, updating failed. (CSCuu99337)
- Resolved an issue where the system did not acknowledge users as members of their primary LDAP groups. (CSCuv03821)
- Resolved an issue where, if you generated a connection event report and modified the **Maximum Results** value, the system did not save the new value and generated the report with the default value. (CSCuv06557)
- Resolved an issue where, if you configured the system to use a remote NTP server to synchronize time to a system with a managed device running a version older than Version 5.4 and you experienced a leap second, your system used a high amount of CPU. (CSCuv11738)
- Resolved an issue where, if you created an access control rule configured with an Interactive Block action and you viewed a blocked webpage in a Chrome web browser, the **Continue** button to bypass the block page did not work. (CSCuv21748)
- Resolved an issue where generated internal CA certificates were valid for only 30 days instead of 10 years. (CSCuv29004)
- Resolved an issue where, if a host generated an Indication of Compromise (IoC) and you disabled the IoC for that host on the Host Profile page, the Indications of Compromise by Host dashboard widget incorrectly displayed the IoC when it should not. (CSCuv41376)
- Resolved an issue where, if you created an SSL policy default action set to **Decrypt - Known Key** or **Decrypt - Resign** on a 7000 Series or 8000 Series device and you choose to resume the SSL session with a different source IP address, SSL inspection failed and the connection log displayed an incorrect SSL policy default action. (CSCuv48689)
- You can now view server names and association classification through the `show ntp` CLI command on your Firepower Threat Defense devices. (CSCuv57818)
- Improved file detection and blocking. (CSCuv59181)
- To suppress IPv6 router advertisement messages on a Firepower Threat Defense device, clear the **Enable RA** checkbox in the Settings page (**Device > Device Management > Interfaces> IPv6 > Settings**) under the device interface configuration on the Firepower Management Center. (CSCuv62594)
- Improved memory utilization for port ranges in access control rules. (CSCuv64114)

- Resolved an issue where, if you registered many devices or configured many interfaces on a managed device or created many VPN deployments, the system did not generate information for all of the devices or interfaces or VPN deployments on their respective pages. (CSCuv76287)
- Improved Health Monitor alerting. (CSCuv96121)
- Resolved an issue where merging intrusion policy layers generated errors. (CSCuw34380)
- Improved email notification reliability. (CSCuw36354)
- Resolved an issue where, in some cases, the system experienced errors caused by invalid username values. (CSCuw39725)
- Resolved an issue where, if you switched from Serial Over Lan (SOL) to Lights-out-Management (LOM) on a MC4000, or vice versa, the system's console port did not work. (CSCuw67319)
- Resolved an issue where, if you enabled SSL debug logging via the `system support ssl-debug` or `system support debug-DAQ-NSE` CLI command and your system experienced a high amount of traffic for an extended amount of time, the system experienced disk space issues. (CSCuw68004)

Known Issues

You can view known issues reported in this release using the Cisco Bug Search Tool (https://tools.cisco.com/bugsearch/). A Cisco account is required.

The following known issues are reported in Version 6.0.1:

- The system allows you to select a custom context on the ASA FirePOWER Configuration page (**Configuration > ASA FirePOWER Configuration**) of an ASA Firepower module managed by ASDM running Version 6.0.1 even though custom context is not supported on devices managed by ASDM. Cisco strongly recommends using admin context on the ASA FirePOWER Configuration page. (CSCus71713, CSCuy18360)
- In some cases, the system takes several minutes or longer to save and update the base layer of an intrusion policy. (CSCux00181)
- The system may experience dropped packets if you edit the access control policy to an intrusion preventative default action and deploy to registered devices configured with routed, transparent, or inline interfaces. (CSCux02726)
- In some cases, if a 7000 Series or 8000 Series high availability pair and the Firepower Management Center experiences a disruption in communication, you cannot break the high availability pair. If you cannot break a high availability pair, contact Support. (CSCux18768)
- In some cases, if you enable a field in a network analysis (NAP) policy that is blank by default and enter a custom value, deploying the NAP policy fails. (CSCux32261)
- Version 6.0.1 does not support 2-byte characters in correlation policy names. If you use 2-byte characters in the name of a correlation policy and deploy, the system does not correctly apply the correlation rule. (CSCux35635)
- You are able to use non-numerical characters as IP addressed in the IPv4 or IPv6 Prefix List when you should not. If you use non-numerical characters for the Prefix List and include the Prefix List, deploy fails. (CSCux40496, CSCux40499)
- If you manage a Firepower Threat Defense Virtual (VMware or Amazon Web Services (AWS), or a Firepower Threat Defense Virtual in a high availability pair, the License page (**System > License**) displays an incorrect number of licenses applied to virtual devices. (CSCux42926, CSCux78687)
- In some cases, if you deploy to a high availability device pair and switch peers, the system incorrectly marks the access control policy as out-of-date when it is not. As a workaround, switch the peers of a registered high availability pair and save, then edit the access control policy and deploy. (CSCux47354)
- In some cases, if you register an ASA Firepower module to the Firepower Management Center and add a production license on the Register page (**System > Licenses > Smart Licenses > Register**), the system generates a `Failed to parse the message sent from the server` error and you cannot deploy the production license. As a workaround, select the evaluation mode license and deploy. If the system continues to experience errors after deploying the workaround, contact Support. (CSCux48513)

- The system does not generate a warning to remove local users if you enable shell authentication with external authentication when it should. (CSCux52235)
- You cannot delete multiple devices registered to a subdomain while editing the Domains page (**System > Domains**). As a workaround, click edit the domain page and save, then edit the domain again and delete the devices removed. (CSCux56021)
- In some cases, if the update fails while updating an ASA with Firepower Threat Defense to Version 6.0.1 and you resume the update, the access control policy is not marked as-of-date when it should. As a workaround, edit the access control policy and save, then redeploy. (CSCux63806)
- Right-clicking an intrusion rule on the Intrusion Rules page (**Objects > Intrusion Rules**) does not generate the context menu does when it should. As a workaround, right click an intrusion rule from the intrusion Edit Policy page (**Policies > Access control > Intrusion > Rules**) to use the context menu. (CSCux64452)
- If you check **Enable HTTP Server** and **Add** an HTTP configuration to the HTTP section in the Platform Settings policy page (**Devices > Platform Settings**) and save, the system generates a `Please make sure HTTP server is enabled. Press 'Yes' to continue` error regardless of whether **Enable HTTP Server** is checked or not. (CSCux67336)
- In some cases, if you edit a file policy, a DNS policy, an identity policy, or an intrusion policy that is referenced in an access control rule on a system running at least Version 6.0, the deploy notification window does not display the correct time when you modified or added the referenced policies. (CSCux74589)
- In some cases, if you deregister an ASA Firepower module from a Firepower Management Center and switch the device to an ASA FirePOWER device managed by ASDM, then create and deploy an access control policy containing web application conditions, deployment fails. As a workaround, install the latest vulnerability database (VDB). (CSCux80311)
- In some cases, if you deploy a file rule with the action set to **Detect Files** or **Block Files** to a device registered to a system running Version 5.4.0.4 or Version 6.0.1, the system may not correctly detect or block the file types, or decompress the archives correctly on the File Summary page (**Analysis > Files > Events**) and the Connection Events page (**Analysis > Connections > Events**). (CSCux81938, CSCux81952)
- In some cases, if the configured NTP server disconnects from the Firepower Management Center, the system incorrectly displays the NTP server as still connected. (CSCux90009)
- If you create an SSL rule and add an Uncategorized URL condition on the Category tab, the rule matches against any URL rather than only matching uncategorized URLs. (CSCux94309)
- In some cases, if you edit and deploy an access control rule with logging enabled, then edit the same access control rule, the system incorrectly displays logging as disabled within the rule. View the Logging tab of the access control editor to review the correct logging configuration. (CSCux94318, CSCuy13079)
- The following system-provided network objects are not included in the drop-down list on the Object Management page (**Objects > Object Management**): `any`, `any-ipv4`, and `any-ipv6`. (CSCux94621)
- Although the configuration options for Firepower Management Center high availability appear in the Integration page of the user interface, high availability is not supported for Firepower Management Centers in this release. Do not attempt to place Firepower Management Centers into high availability. (CSCuy96369)
- If you add a routed IPv6 IP in the Devices tab of the Device Management page (**Devices > Device Management**) of an ASA with Firepower Threat Defense and enable an IPv6 Prefix without checking the **Enable Router Advertisement** option, then save and deploy, deployment fails and the system generates a `Deployment failed due to configuration error. If problem persists after retrying, contact Cisco TAC.` error. As a workaround, check the **Enable Router Advertisement** option and redeploy. (CSCux98850)
- In some cases, if you deploy an access control rule with the default action set to either **Interactive Block** or **Interactive Block with Reset** to a registered ASA Firepower running Threat Defense in a high availability pair and then manually switch the active peer in the high availability pair, the interactive block page does not proceed after you click **Continue**. Click **Continue** a second time to bypass the interactive block page. (CSCux99397)
- Viewing files containing the .JPEG extension in Version 6.0.1 generates a `HTTP 403 Forbidden error` page. You can correctly download and view files containing the .jpg extension. (CSCux99481)

- In some cases, if you view the Identity Services Engine (ISE) section of the Identity Sources tab in the Integration page (**System > Integration**), then upload a Firepower Management Center server certificate with the corresponding key and name the certificate, the save button does not operate. As a workaround, exit the Firepower Management Center certificate window and click the add (+) icon, then save. (CSCux99516)
- In some cases, if you deploy a file policy with **All types in selected Categories** selected as the file type and enable the local analysis module, the file composition report of a detected file incorrectly displays the MD5 value as `00000000000000000000000000000000`. (CSCuy01702)
- In some cases, if you attempt to simultaneously register two devices and deploy policy configurations on a Firepower Management Center, the system may generate a `Pre-deploy Global Configuration Generation. _storePerms: Unable to store perms` error in the Tasks tab of the Message Center. As a workaround, redeploy policies. (CSCuy02038)
- If you create an SSL policy containing one SSL rule with the action set to a **Decrypt-Known Key** and a second SSL rule with the action set to **Decrypt-Resign** a on a system running Version 6.0.1, the system incorrectly generates an erroneous `Warning: this rule is preempted by rule <second rule listed>` warning. (CSCuy03840)
- If you view a global domain access control rule of an access control policy in a subdomain and add or edit an access control rule in any other policy, the system incorrectly disables the logging options in the Logging tab of the rule editor window. As a workaround, refresh the page. (CSCuy03909)
- If you create an access control policy on a system running Version 6.0. or earlier and update the system to Version 6.0.1, then edit the access control policy, the system does not save the modifications. (CSCuy04151)
- In some cases, if you edit security zones of a Cisco ASA with FirePOWER Services and attempt to deploy configuration from the Device Management page (**Devices > Device Management**), the deploy window does not display any registered devices to deploy to when it should. As a workaround, redeploy the platform settings policy before deploying configuration from the Device Management page. (CSCuy05635)
- If you create an access control rule and select a port to **Add to Destination** in the port tab of the Add Rule window, the system does not let you select the same port and **Add to Source**. As a workaround, if you need to use the same port as both a destination port and a source port, **Add to Source** before you **Add to Destination**. (CSCuy08262)
- If you add a user to a new access control rule via the Users tab of the Add Rule window and edit the same access control rule to add another user from, then attempt to delete the first user in the Selected Users column, the system incorrectly removes the wrong user from the Selected Users list. As a workaround, delete required users before adding new user to the selected list. (CSCuy08275)
- The Firepower Management Center may experience a moderate delay in response time or system issues if you register and manage more than 100 devices at a time. (CSCuy12452)
- The system incorrectly allows you to configure **Do not calculate SHA256 hash values for files larger than** value to be smaller than the **Maximum file size for dynamic analysis testing** value in the File and Malware Settings section in the Advanced tab of the access control policy. To ensure the system is operating at maximum efficiency, please configure the **Do not calculate SHA256 hash values for files larger than** value to be smaller than the **Maximum file size for dynamic analysis testing** value. (CSCuy13054)
- The Device Management page (**Devices > Device Management**) and the Appliance Status section of the Health Monitor page (**System > Health > Health Monitor**) incorrectly displays the configured IP address as the name of a registered ASA Firepower device running Threat Defense. (CSCuy13451)
- In some cases, if you remove a whitelist or blacklist entry on the global whitelist or global blacklist page (**Security Intelligence > Network Lists and Feeds > Global Whitelist** or **Global Balcklist**) and save changes via the Chrome web browser, then try to edit the global whitelist or blacklist again, the system does not let you edit the whitelist or blacklist again. As a workaround, refresh the page to edit the whitelist or blacklist. (CSCuy14441)
- If you edit an access control rule with the action set to **Monitor**, **Trust**, **Block**, or **Interactive Block with Reset** and deploy changes, the system erroneously generates a `Selecting this action will reset the Intrusion Policy and File Policy to "None". Are you sure you want to continue?` warning whether the access control policy contains an intrusion policy and a file policy or not. Close out the warning message to deploy changes. (CSCuy14455)
- If you query `CISCO-MEMORY-POOL-MIB` or `CISCO-ENHANCED-MEMPOOL-MIB` on a Cisco ASA with FirePOWER Services or Firepower Threat Defense, the ASA may experience high CPU utilization. (CSCuy14724)

- In some cases, the Firepower Management Center does not display all health events generated from registered Firepower Threat Defense devices. (CSCuy16548)
- In some cases, if you create an access control rule containing an web application condition or an application risk level and **Store ASA FirePOWER changes** on an ASA Firepower managed by ASDM, the system generates a `Policy has rules with missing detectors. The following rules specify applications for which a detector is not defined` error and does not save changes. (CSCuy18141)
- In some cases, if the system continuously receives large amounts of Microsoft Active Directory user sessions and the network map experiences issues, and detected user sessions are not mapped to realms. If the system experiences issues mapping detected users to realms, contact Support. (CSCuy18154)
- In some cases, you are unable to edit a recently modified Intrusion policy under the Inspection tab of the Editing Rule window (**Policies > Access Control > Access Control Rules**). (CSCuy18430)
- In some cases, if you create and enable a realm on an ASA FirePOWERdevice managed by ASDM, then click **Download** on the User Download tab of the Realm Editor page prior to adding the ASA FirePOWER device managed by ASDM IP address to a supported Windows server, the device CPU experiences high volume when it should not and may encounter communication delays. (CSCuy18523)
- If you deploy a custom network list to devices registered on a subdomain and then move the device to another leaf domain, deploy fails. As a workaround, use a system-provided network list prior to moving the device from a subdomain to a leaf domain. (CSCuy19978)
- The **Syslog ID** drop-down list of the Syslog Settings pop-up window does not list all the supported Syslog IDs if you edit the Syslog Settings page (**Devices > Platform Settings > Syslog > Syslog Setting**). (CSCuy21648)
- If you edit an intrusion policy and click one of the categories listed in the Classifications section of the Rules window on the Edit Policy page (**Policies > Access Control > Intrusion**), the system does not display all the relevant rules when it should. (CSCuy22305)
- In some cases, if you access the Firepower Management Center web interface via an IPv6 address with Internet Explorer version 11, the web interfaces experiences a slow response time. As a workaround, either use a different web browser or use an IPv4 address. (CSCuy22566)
- In rare cases, if you deploy a VPN on a 7000 Series or 8000 Series device that experiences issues and the system generates health alerts in the Health tab of the Message Center, then you delete the VPN, the system continues to generate health alerts for the VPN even though the configuration is deleted. Once the VPN configuration is removed, the alerts have no impact on device functionality. (CSCuy25356)
- In some cases, accessing the online help page (**Help > ASA Firepower Online Help**) on an ASA Firepower managed by ASDM incorrectly generates an `Error - 403 Forbidden You have tried to access a page that is forbidden` error. (CSCuy27084)
- In some cases, if device registration to a Firepower Management Center fails, the **Create new policy** option on the Add Device page does not respond. As a workaround, **Add Device** again. (CSCuy28275)
- If you expand the **SSL Policy to use for inspecting encrypted connections** option under the SSL Policy Settings section of the Advanced tab on the Access Control Policy page (**Policies > Access Control**) and click the help icon, the system incorrectly generates a `Error 404:page not found page` error. (CSCuy28935)
- If you click the help icon in the Compare Policy window of the Access Control policy page (**Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**) on an ASA FirePOWER device managed by ASDM, the system does not redirect to the help page when it should. (CSCuy28937)
- If you **Add URL** on the URL tab of the Object Management page (**Configuration > ASA FirePOWER Configuration > Object Management**) of an ASA FirePOWER device managed by ASDM and use unsupported characters in the name of the URL, the system does not generate an error message when it should. The following characters are currently supported: (**a...z**), (**A...Z**), (**-**) (**_**) (**+**) (**.**). Note that the URL object name must start with a letter or an underscore (**_**). (CSCuy28945)
- If you deploy an SSL rule with the rule action set to **Decrypt-Resign** and browse decrypted websites using Chrome Version 40 or later, the browser generates alerts for the decrypted websites. As a workaround, use the Internet Explorer or Firefox web browser. (CSCuy30988)

- In some cases, if the active peer of a high availability pair of ASA Firepower devices running Threat Defense uses all available disk space and the system automatically switches the backup peer as the active peer, then you free up disk space on the backup peer and manually switch the backup peer with the active peer, the Tasks tab of the System Alerts page erroneously reports the high availability switch taking several minutes to complete. (CSCuy31838)
- The system does not alert you to click the **Refresh** icon on the User Download tab of the Realms editor page (**Configuration > ASA FirePOWER Configuration > Integration > Realms**) if you modify the Group DN option in the Realm Configuration tab of the Realms page when it should. (CSCuy32051)
- In some cases, if you deploy an access control policy referencing an intrusion policy and an SSL with the action set to **Decrypt-Resign**, the system does not generate downloadable packet information on the packet view of the Intrusion Events page (**Analysis > Intrusion > Events**). (CSCuy34078)
- If you create high availability pair with two ASA with Firepower Threat Defense devices and the active peer in the high availability pair does not have any settings configured on the Platform Settings page (**Devices > Platform Settings**), then click **Policy Assignments**, the system does not display the high availability pair as an available device to deploy to. As a workaround, configure platform settings to both ASA with Firepower Threat Defense devices prior to creating the high availability pair. (CSCuy35753)
- In some cases, if you modify and deploy a rule from the packet view, the web page generates a `HTTP Error 500 Internal server error` page. (CSCuy36187)
- In some cases, if you edit the global blacklist and deploy configuration, the system marks the access control policy as out-of-date when it should not. As a workaround, redeploy. (CSCuy36653)
- The system displays incorrect egress or ingress interface names for processed traffic in the Connection Events page (**Configuration > ASA FirePOWER Configuration > Eventing**) and you cannot filter traffic by egress or ingress interface names on ASA FirePOWER managed by ASDM with multiple contexts. (CSCuy36674)
- If you remove a user from all groups within a realm referenced in the access control policy and deploy configuration changes, then click **Download users and groups** from the Access Control tab, the system does not update the deployed configuration and continues to process traffic as if the group(s) still contained the user. (CSCuy39685)
- In rare cases, deploying configuration fails and the system generates a `Deployment failed in policy and object collection. If problem persists after retrying, contact Cisco TAC`. error when it should not. As a workaround, redeploy configuration. (CSCuy36942)
- The **State** column of the Application Detectors page (**Policies > Application Detectors**) does not sort the application detector table when it should. (CSCuy41052)
- The table view of the Connection Events page (**Analysis > Connections > Events**) does not display values for the Initiator User column when it should. (CSCuy41300)
- In some cases, if you open the Add Neighbor window from the BGP IPV4 Routing tab of the Device Management page (**Devices > Device Management)** of a registered device running Firepower Threat Defense and check the **Configure Graceful Restart** option, deploying to a Firepower Threat Defense high availability pair fails. As a workaround, do not enable the **Configure Graceful Restart** option. (CSCuy41385)
- If you check more than one event from the table view of the Reviewed Events page (**Analysis > Intrusions > Reviewed Events**) and click **View All**, the generated packet view incorrectly displays one of the checked events instead of all the checked events. (CSCuy42838)
- In some cases, if you deploy an access control rule and set the rule action to **Allow** or **Block** a port object network condition of **ICMPv6 Type 2** with codes `0-255`, the system allows all network condition types even if the rule is configured to **Block**. (CSCuy43967)
- In some cases, if you use the Chrome web browser to access the Firepower Management Center and add either an object or a group from the Add VLAN Tag drop-down list two consecutive times or more on the VLAN Tag page (**Objects > VLAN Tag**), the system does not generate the **Add Object** or **Add Group** window. If you attempt to delete an object or group from the VLAN Tag page, the system generates an `An internal error occurred` error. As a workaround, use either Internet Explorer or Firefox browsers. (CSCuy44276)

- In some cases, attempting to create or delete 1000 alerts generates a `Authorization Failure: Invalid or expired session (code = 0) at /usr/local/sf/lib/perl/5.10.1/SF/EOHandler.pm line 3212` error. (CSCuy45377)
- In some cases, if you create a system policy and enable SNMP **Version 3** under the Access List tab of the Platforms Settings page (**Devices > Platform Settings**), then add a user to the SNMP window and click **Save**, the system generates a `This policy includes access to pot 161 (snmp), but no SNMP users have been added.` error and you cannot save the policy with SNMP settings. As a workaround, click either SNMP **Version 1** or **Version 2**. If you must use SNMP **Version 3**, add SNMP users before selecting the SNMP version and save, then enable port access in the Access List tab of the Platforms Settings page and save. (CSCuy46080)
- If you add SNMP access to an ASA Firepower managed by ASDM on the System Policy page (**Configuration > ASA FirePOWER configuration > Local > System Policy**) and select **Version 3** from the SNMP Version drop-down list, then **Add User** and expand the Authentication Protocol drop-down list, the system does not generate any options. (CSCuy46264)
- If you right click in the Networks tab of the Network Discovery page (**Policies > Network Discovery**), the system incorrectly generates the context menu even if a rule is not selected. (CSCuy46940)
- In some cases, if you configure transparent inline mode or passive mode on a registered device and deploy an intrusion rule, the system does not generate VLAN tags for all traffic types in the expanded packet view of the Intrusion Events page (**Analysis > Intrusion > Events**). (CSCuy47287)
- In some cases, if the system experiences a failover, the rate of transferring HTTP traffic may slow down. (CSCuy47595)
- If you view the web interface via the Chrome web browser, the system may not allow you to **Add Security Zon**e or edit an existing security zone of a registered NGIPSv device from the Security Zone tab of the Object Management page (**Object > Object Management > Security Zone**). As a workaround, reload the current page or use a different web browser. (CSCuy48328)
- If you import an internal certificate on the Object Management page (**Object > Object Management**) and cancel the Import Internal Certificate Authority window before saving the certificate, then attempt to import the same internal certificate, the system generates the Import Internal Certificate Authority window but does not display any information in the window and you cannot import the certificate. (CSCuy49034)
- In some cases, if deploy an intrusion rule containing an **AppID** web application condition and the system detects an HTTP session followed by an FTP session, the system incorrectly categorizes the FTP session as an HTTP session and experiences issues. (CSCuy49662)
- In some cases, the system does not display intrusion rules deployed at the Global domain in the expanded packet view of the Intrusion Events page (**Analysis > Intrusion > Events**). (CSCuy49667)
- If you create a cluster of the following ASA FirePOWER Services devices, the system does not dispaly the correct cluster icon on both the Deploy dialog window or the Device page: The ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, or the ASA 5585-X-SSP-60. (CSCuy51025)
- In some cases, if you create a syslog alert and the system experiences issues, the system generates extraneous health alerts about enabled detection engines. As a workaround, disable the syslog alert and deploy configurations. (CSCuy51339)
- In some cases, if you break a 7000 Series or 8000 Series high availability pair, the system keeps the high availability configuration in the deployments tab of the System Alerts screen when it should not. (CSCuy51614)
- If you check the **Enable Auto Update**s option in the Import Rules page (**Objects > intrusion Rules > Import Rules**), the system incorrectly defaults to an invalid value. If you **check Enable Auto Updates**, you must manually set the auto update minutes value. (CSCuy51949)
- In rare cases, if you reconfigure multiple domains or traffic profiles and delete a domain while changes are saving, the system experiences issues. As a workaround, wait until configurations are saved and deployed before deleting a domain. (CSCuy54834)
- In rare cases, you may experience issues or delays in event processing after deleting a domain. (CSCuy58101, CSCuy60808)
- In some cases, leaving a Firepower Management Center Virtual connected the Cisco cloud may cause system issues. (CSCuy56120)

- In some cases, the system stops added new hosts to the network map and the host view of the Discovery Event page (**Analysis > Hosts > Discovery Events**) incorrectly displays the host limit has been reached. (CSCuy57044)
- In some cases, if you break a Firepower Threat Defense high availability pair, one of the devices in the pair stays in standalone mode and the system cannot recreate the high availability pair. (CSCuy57756)
- If you view the web interface in Japanese, the **Save** button on the VMware Tool page (System > VMware Tool) is not translated when it should. (CSCuy58426)
- If you view the web interface in Japanese and click **Deploy** from the Policies page and view the deploy window, the **Cancel** button in the deploy window is not translated when it should. (CSCuy58661)
- In some cases, updating the Firepower Management Centerr to Version 6.0.1 via the Chrome web browser causes policy pages to load slowly. As a workaround, use either the Firefox or Internet Explorer web browsers. (CSCuy58664)
- In some cases, if registered ASA devices with Firepower Threat Defense or ASA Firepower modules experience bursts of high volume of traffic, device interfaces processing incoming traffic drops packets and the CPU does not appear to experience high usage. (CSCuy59642, CSCuy66405)
- If you deploy a NAP policy with **Max Detect** selected as the base policy, the system only deploys the policy to registered ASA devices with Firepower Threat Defense. As a workaround, if you must deploy a NAP policy with **Max Detect** selected as the base policy, click the **Add A Layer** option and disable the following options prior to deploying: **Decompress SWF file (LZMA)**, **Decompress SWF File (Deflate)**, and **Decompress PDF File (Deflate)**. (CSCuy60390)
- The **Identify as Special Identities/Guest if authentication cannot identify user** checkbox in identity rule configuration is incorrectly named. It should be named **Identify as Guest if authentication cannot identify user**. (CSCuy65461)
- If you click **Add Task** on the Scheduling page (**Configuration > ASA FirePOWER Configuration > Tools > Scheduling**) of an ASA device managed by ASDM and view the values displayed in the time drop-down list, the web interface incorrectly colors the values red and the values are not fully visible. (CSCuy69547)
- The Firepower Management Center cannot successfully deploy configuration to a Firepower Threat Defense high availability pair using an EtherChannel connection as the LAN failover link, and attempting to break the high availability pair may fail.(CSCuy73041)
- If you edit a device registered in a leaf domain from the Global domain while using Internet Explorer version 11, the system does not redirect you to the device edit page when it should. As a workaround, edit the device in the domain it is assigned to. (CSCuy73776)
- In some cases, if you create an access control rule and add a base policy in the **Inheritance Settings** window in the Security Intelligence tab of Initial Access Control Policy page (**Policies > Access Control > Access Control**), then check the **Inherit from base policy** option, the system does not let you uncheck the Inherit from base policy option. As a workaround, remove the inherited base policy from the access control rule and save, then add the base policy in the **Inheritance Settings** window again. (CSCuy74319)
- If you update a Cisco ASA with FirePOWER Services to Version 6.0.1 and attempt to deploy policies via ASDM, policy deployment may fail. As a workaround, download and apply the latest SRU from the Support site or add the device to a Firepower Management Center and deploy the policy from the Firepower Management Center. (CSCuy84095)

The following known issues were reported in previous releases:

- You may experience latency if you use Firefox version 38.0.1 to view your Firepower Management Center's interface. As a workaround, use Firefox 41 or later or use a different web browser. (CSCuv11830)
- In some cases, if you create an access control policy when registering a device on a subdomain, the system creates the access control policy in the global domain instead of the subdomain when it should not. (CSCut56951)
- In some cases, if you edit a route map from **Allow** to **Block** on a Firepower Threat Defense device, the system does not deploy the edit to your managed devices. As a workaround, create a new route map on the Route Map page (**Objects > Object Management > Route Map**) with the correct action and redeploy. (CSCuu27697)
- In some cases, if you edit the default network access policy in the advanced tab of the Access Control page (**Policies > Access Control**), the system incorrectly displays the default network access policy as an intrusion policy on the deployment dialog window. (CSCuv48221)

- Online help does not open if you click the help icon on the Select Comparison page (**ASA FirePOWER Configuration > Policies > Files > Compare Policies**) of an ASA Firepower module managed via ASDM. (CSCuw21863)
- In some cases, if you view **All Events (Not Dropped)** in the Intrusion Events table view page of a Firepower 7000 Series or 8000 Series device and sort the table by a maximum of six fields including **Review By** and **Count** and then generate a report, report generation fails. As a workaround, exclude either the **Review By** and **Count** field values or, if you include both the **Review By** and **Count** fields, only nor more than three additional field values when generating a report from the intrusion events page. (CSCuw29993)
- You cannot name a device group with a name that includes the plus (`+`) character even though the system generates a `This field contains invalid characters. Only alphanumerics, hyphen ( - ), underscore ( _ ), period ( . ), and plus ( + ) are allowed` message. (CSCuw44373)
- In some cases, if you edit the browser and shell timeout threshold values on the Shell Timeout page (**System > Configuration > Shell Timeout**) and redeploy, the system logs out of inactive Firepower Management Centers up to one minute after the configured threshold values. (CSCuw48568)
- In some cases, editing a file list in a domain causes any file policy in that domain to be marked out-of-date. (CSCuw52764)
- The Device Management page (**Devices > Device Management**) does not display device override values in the tooltip for device objects. (CSCuw53371)
- External certificates from Version 5.4.x are not supported in Version 6.0: the only curves supported in Version 6.0 are `prime192v1`, `prime256v1`,`secp384r1` and `secp521r1`. You must update your system to Version 6.0 to obtain supported external certificates. (CSCuw54749)
- In some cases, if you create an access control policy referencing both a file policy containing a file rule configured to **Detect Files** and an SSL policy configured to **Decrypt--Resign** or **Decrypt--known key** on a system sending and receiving emails with Outlook 2013, the Connection Events page (**Analysis > Connections > Events**) does not include email file attachments in generated events. (CSCuw65152)
- In some cases, if you refresh the tabs in the Device Management page (**Devices > Device Management**) or the NAT page (**Devices > NAT**) or the VPN page (**Devices > VPN**), the system does not clear the cache on the page being refreshed and the **Save** button is un-operational. As a workaround, cancel any edits made to the page or tab and select the device you want to edit again. (CSCuw75367)
- In some cases, if you create an SSL policy containing a certificate with more than one status, such as expired or revoked, the Certificate Status column of the Connection Events page (**Analysis > Connections > Events**) does not display a status. (CSCuw76040)
- In rare cases, if you create or edit a device interface on the Device Management page (**Devices > Devices Management**), the system generates a `No cache exists to discard and resume` error and you cannot deploy. As a workaround, refresh the Device Management page and redeploy. (CSCuw77505)
- In some cases, if you incorrectly configure OSPFv3, RIP or Border Gateway Protocol on a device's virtual router page (**Devices > Devices Management > Virtual Router**) and leave the configuration page without saving changes, the system generates a **To revert back the configuration** pop-up; click **Yes** to clean the virtual router configuration page of any edits or click **No** causes the system to generate the **To revert back the configuration** pop-up multiple times before saving the virtual router configuration page without any edits. (CSCuw78916)
- If you deploy a network discovery policy to a Firepower 9300 cluster or clustered or stacked Firepower 7000 Series or 8000 Series devices (in Version 6.0 known as a high availability pair), the system incorrectly counts all devices in the cluster or stack rather than indicating one device for the cluster or stack. (CSCuw79241, CSCuw79243)
- If you want to reimage your ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, or ASA 5516-X device to Firepower Threat Defense, you must verify your ROMMON image meets the recommended version, Version 1.1.8, prior to reimaging. For more information on reimaging to Firepower threat Defense, see the *Cisco Firepower Threat Defense Quick Start Guide*. (CSCuw79771)
- After initial setup on a Firepower Management Center, Firepower 7000 Series, or 8000 Series device, if you are connecting to the appliance from behind a network address translator (NAT) device, the system provides a redirect URL containing the IP address for the IP address you configured for the appliance rather than the NAT IP you are connecting to, and the session times out. As a workaround, correct the URL to use the NAT IP used to connect via web. (CSCuw79967)

- If you uninstall Version 5.4.1.3 or later to an earlier 5.4.x version and then update the system to Version 6.0, the update to Version 6.0 fails. Update your system to the latest version prior to updating your system to Version 6.0. (CSCuw81780)
- In some cases, if you do not select the required licenses for a device prior to device registration, the system generates an `Initial policy deployment not started due to validation errors. For details, redeploy manually` message. For more information on the correct licenses to select for your device, see the Licensing the FireSIGHT System chapter of the *Firepower Management Center Configuration Guide*. (CSCuw85743)
- If you edit a Firepower Threat Defense interface to use a static route IPV6 address for either a network or gateway IP address that has already been configured, the system allows you to do so even though the configuration is invalid. (CSCuw87053)
- When configuring OSPFv3 routing settings on a Firepower Threat Defense device, if you configure redistribution using a route map that is not used elsewhere in the device configuration, then delete the redistribution, deployment fails. As a workaround, either remove a route map first & deploy or configure use of the same route map elsewhere before deleting the OSPFv3 redistribution configuration. (CSCut87162)
- In some cases, if you deploy a NAT policy containing rules targeted to Firepower 7000 Series or 8000 Series managed devices' routed interfaces and then cluster the managed devices (known is Version 6.0 as a high-availability pair), some NAT rules continue to target a managed device's routed interface instead of changing to target a high availability interface when it should. As a workaround, edit the rule containing the individual interface, manually create a high availability interface, then redeploy. (CSCuw89223)
- The HTTP Listing page (**Device > Platform Settings > Firepower Threat Defense Platform Settings > HTTP**) lists **Authentication Certificate** as a configurable field when it is not. (CSCuw89605)
- In some cases, the system generates events for large amounts of HTTP traffic processed by a port that is not specified in the HTTP preprocessor rule. As a workaround, add the port to the HTTP preprocessor rule with GID `119` and SID `15`. (CSCuw90033)
- If you initiate deployment while backing up the Firepower Management Center, a message does not appear to indicate that the communication channel is blocked and the policy cannot deploy. Wait until backup process is complete and then deploy. (CSCuw90629)
- In some cases, if you create an access control policy that has an intrusion policy as the default action, the variable set icon next to the default action does not display properly. As a workaround, change the default action to use a different intrusion policy, which makes the icon show up, and then change your default action back to the previous intrusion policy. (CSCuw94067)
- In some cases, the Firepower Management Center's Deploy window displays an incorrect timestamp after you update the Firepower Management Center to Version 6.0 and deploy configuration changes. (CSCuw94083)
- In some cases, if you create an OSPFv3 router but do not configure a manual router-id in the Advanced Settings tab of the router page (**Devices > Device Management > Router**), the system does not use unnamed IPv4 IP addresses and generates an `OPSFv3 router process will not start as no router ID has been configured. Neither router ID in OSPFv3 nor IPv4 address configured in Interfaces` error message. (CSCuw95485)
- If you create a correlation rule configured to match a **MAC Vendor is** condition, the system generates a `Warning: no vendors match this string` warning and does not execute the correlation rule. As a workaround, update your vulnerability database (VDB). If the VDB update does not resolve the issue, use the **MAC Vendor contains** condition instead of the **MAC Vendor is** condition. (CSCuw96022)
- The link to the Cisco Smart Software Manager from the Firepower Management Center Smart Licensing user interface page (**System > Local > System Policy**) directs to an updated link, which also redirects. As a workaround, if the redirect does not occur quickly enough, connect to https://software.cisco.com/#module/SmartLicensing. (CSCuw96552)
- In some cases, deploy fails on a device running Version 5.4.0 that is registered to a Firepower Management Center running Version 6.0 if you deploy an access control policy that references a file policy configured for malware protection. (CSCuw97809)
- In some cases, if you enable sensitive data detection in the Advanced Settings on the Intrusion Policy page (**Policies > Intrusion > Intrusion Policy**), then switch to another domain before saving, the system does not reload the Intrusion Policy page in the destination domain when it should. As a workaround, save or manually reload the Intrusion Policy page. (CSCuw97864)

- In some cases, if the time configured on a device running Version 6.0 is set ahead of the time configured on a Firepower Management Center, registering the managed device to the Firepower Management Center causes connectivity issues and the system may not be able to restore connectivity. As a workaround, execute the `/etc/rc.d/init.d/pm restart` CLI command. If you continue to experience connectivity issues, contact Support. (CSCuw97948)
- The `system shutdown` CLI command causes ASA Firepower modules (ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X) running Firepower Threat Defense to restart instead of shut down. (CSCuw98231)
- In some cases, if your user interface initiates a restore, the session will be disconnected and you must log in again to see the status of restore operation. (CSCuw98296)
- Version 6.0 does not support the Safari web browser on systems running the MAC OS. Use Firefox, Chrome, or Internet Explorer. (CSCuw98876)
- In some cases, if the system hosting a virtual device experiences a high amount of traffic, deploying to the virtual device may cause temporary network issues. (CSCux00380)
- In some cases, intrusion events do not display the correct source IP address or the correct destination IP address. As a workaround, view the Connection Events page (**Analysis > Connections > Events**) to view the correct source and destination IP addresses of an intrusion event. (CSCux00385)
- In some cases pinholes are not created for Real-time Transport Protocol (RTP) connections established by calls using the Session Initiation Protocol (SIP), which prevents the VOIP channel creation for the SIP call. (CSCux03758, CSCux09765)
- Although an application detector is available for the Skinny (SCCP) protocol, pinholes are not created for RTP connections established by SCCP packets. (CSCux05468)
- If you enable the **CPU Usage** health monitor on the Health Policy page (**Health > Health Policy**) for a Firepower Threat Defense device, the device generates transient erroneous 100% CPU load alarms during deployment. (CSCux07384)
- In some cases, if you create a Firepower Threat Defense device in transparent mode and register the device to a Firepower Management Center, then assign an IP address to an interface being used as the device's diagnostic interface, the Firepower Management Center does not successfully deploy the assigned IP address to the Firepower Threat Defense device. Cisco recommends restarting the Firepower Threat Defense device for the changes to take effect. (CSCux07416)
- In some cases, if you only edit the logical device's management interface of a Firepower 9300 device and deploy, the system does not warn you that the device must reboot to deploy changes when it should. (CSCux07831)
- In some cases, when deploying policies to a large number of devices, policy deployment times out and fails when Snort fails to restart. (CSCux07861)
- Rarely, during booting of the Firepower 9300, it may fail to initialize and become operational. When this happens the device will automatically reboot. No interaction is required, the device will become operational after the successful boot attempt. (CSCux07881)
- In some cases, if you deploy a clustered Firepower Threat Defense device and attempt to move the device from one subdomain to another subdomain, moving the device fails and the system generates an `Updating Domain management changes failed` error message. (CSCux08012)
- In some cases on Firepower 9300, if one of the nodes fails a health check during a deployment, the node is separated from the configured cluster and deployment to the cluster fails. Such a situation is recoverable on its own and when the node re-joins the cluster, retry deployment. (CSCux08115)
- In the Firepower 9300 Chassis Manager, you may not be able to edit the interface in the last row on the Interfaces screen. In addition, you may not be able to manually select some interfaces during logical device provisioning from the Chassis Manager. As a workaround, decrease the font size of your web browser. (CSCux08577)
- In some cases, if you create a cluster of Firepower 9300 devices on a Firepower Management Centerand configure interface IP addresses and a translated address pool through the Firepower Management Center user interface, the IP Pool configuration does not deploy to the device if you deploy immediately after configuring. As a workaround, edit the Interface and IP Pool again and redeploy. (CSCux09023)

- If you deploy a NAT policy which resides in a subdomain to a Firepower 7000 Series or 8000 Series device and move the device to new domain, deploy fails. As a workaround, create a new NAT policy in a new domain and target the correct device, then redeploy. (CSCux10651)
- In some cases, if you create a VPN deployment on a registered device and move the device from one domain to another domain, then deploy, deploy fails and the system generates a `Pre-deploy Global Configuration Generation. Cannot find policy information` error message. As a workaround, remove the VPN configuration prior to moving the device to another domain. An alternative workaround is to unregister and then register the device to the Firepower Management Center, then create a VPN deployment and deploy. (CSCux10820)
- Use of a certificate with an RSASSA-PSS signature algorithm on a Firepower Management Centerr is not supported in Version 6.0. If you update a Firepower Management Center using such a certificate to Version 6.0 or add such a certificate in Version 6.0, the system does not allow you to log into the Management Center web interface and generates an `Unable to authorize access. If you continue to have difficulty accessing this device, please contact the system administrator` error. As a workaround, prior to update, generate and install an SSL certificate with either a `sha1WithRSAEncryption` or `sha256WithRSAEncryption` algorithm and restart the Firepower Management Center, or use the default Firepower Management Center certificate and restart the appliance. If you are unable to access the user interface on your Firepower Management Center, contact Support. (CSCux30610)
- If the certificate used by your Firepower Management Center was generated using a public server key larger than 2048 bits, you will not be able to log into the Firepower Management Center web interface after updating to Version 6.0. As a workaround, replace certificates that were created with larger public keys by generating a server certificate request and then applying a certificate generated using that request to the Firepower Management Center. You can do the server certificate request and the certificate upload through the local configuration settings on the Firepower Management Center (**System > Local > Configuration > HTTPS Certificate**). If you generate a certificate without using a CSR from the Firepower Management Center, use a public key of 2048 bits or less. If you generate a certificate that contains more than 2048 bits and lose access to the Management Center web interface, contact Support. (CSCux35430)

For Assistance

Thank you for choosing the Firepower System.

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information about the Firepower System, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

If you have any questions or require assistance with the Firepower System, please contact Cisco Support:

- Visit the Cisco Support site at http://support.cisco.com/.
- Email Cisco Support at tac@cisco.com.
- Call Cisco Support at 1.408.526.7209 or 1.800.553.2447.